

ARCTIC
OCEAN

NAVAL LAW REVIEW

VOL. 64



NAVAL LAW REVIEW 2015

ARTICLES

STUXNET AND ARTICLE 2(4)'S PROHIBITION AGAINST
THE USE OF FORCE: CUSTOMARY LAW AND
POTENTIAL MODELS

Lieutenant Andrew Moore, JAGC, USN

DEPARTMENT OF DEFENSE WATER RIGHTS:
A PROPOSED POLICY

Captain Michael T. Palmer, JAGC, USN

"POURING NEW WINE INTO OLD BOTTLES":
UNDERSTANDING THE NOTION OF DIRECT PARTICIPATION
IN HOSTILITIES WITHIN THE CYBER DOMAIN

Lieutenant Commander Christopher P. Toscano, JAGC, USN

INVESTIGATING CIVILIAN CASUALTIES
IN ARMED CONFLICT:
COMPARING U.S. MILITARY INVESTIGATIONS WITH
ALTERNATIVES UNDER INTERNATIONAL HUMANITARIAN
AND HUMAN RIGHTS LAW

Commander Sylvaine Wong, JAGC, USN

BOOK REVIEW

FORCES OF FORTUNE: THE RISE OF THE
NEW MUSLIM MIDDLE CLASS AND
WHAT IT WILL MEAN FOR OUR WORLD

Major Alex M. Straub, ARNG

THE GOOD SOLDIERS

Major Timothy W. Thomas, USA

NAVAL LAW REVIEW

Judge Advocate General of the Navy
Vice Admiral James W. Crawford III, JAGC, USN

Commander, Naval Legal Service Command
Rear Admiral John G. Hannink, JAGC, USN

Commanding Officer, Naval Justice School
Captain Shannon H. Kopplin, JAGC, USN

Editor-in-Chief
Lieutenant Commander Bradley L. Davis, JAGC, USN

Article Editors
Lieutenant Commander Heather Henderson, JAGC, USN
Lieutenant Commander Graham C. Winegeart, JAGC, USN
Lieutenant Commander Jason W. Connors, JAGC, USN
Major Izac E. Ossiander, USMC
Lieutenant Omer Duru, JAGC, USN
Lieutenant John Cella, JAGC, USN
Lieutenant Jonathan M. Hawkins, JAGC, USN
Lieutenant Matthew S. Bartholomaeus, JAGC, USN
Mr. Joseph Fandino
Mr. Cody Churchill
Mr. Jesse K. Posey
Mr. Christopher Burkhalter
Mr. R. Charles DiNunzio Jr.
Mr. Cullan Riley
Ms. Mollie C. Topic
Ms. Karisa Chapa

Publication Specialist
Ms. Doris M. Soares

SUBSCRIPTIONS

Subscription information may be obtained by writing to *Naval Law Review*, Naval Justice School, 360 Elliot ST, Newport, RI 02841-1523. Publication exchange subscriptions are available to organizations that publish legal periodicals.

DIGITAL COPIES

Digital copies of the current *Naval Law Review* and earlier volumes are available at http://www.jag.navy.mil/njs_publications.htm

The *Naval Law Review* encourages frank discussion of relevant legislative, administrative, and judicial developments in military and related fields of law. Views expressed in published articles must be considered solely those of individual authors and do not purport to voice the views of the Judge Advocate General, the Department of the Navy, or any other agency or department of the United States. The *Naval Law Review* is published from appropriated funds by authority of the Judge Advocate General in accordance with Navy Publications and Printing Regulations P-35. This issue of the *Naval Law Review* may be cited as 64 NAVAL L. REV. [page number] (2015). A digital version of the *Naval Law Review* may be found on the world wide web at www.jag.navy.mil.

CONTENTS

Articles, Essays & Notes

STUXNET AND ARTICLE 2(4)’S PROHIBITION AGAINST THE USE OF FORCE: CUSTOMARY LAW AND POTENTIAL MODELS Lieutenant Andrew Moore, JAGC, USN	1
DEPARTMENT OF DEFENSE WATER RIGHTS: A PROPOSED POLICY Captain Michael T. Palmer, JAGC, USN	28
“POURING NEW WINE INTO OLD BOTTLES”: UNDERSTANDING THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES WITHIN THE CYBER DOMAIN Lieutenant Commander Christopher P. Toscano, JAGC, USN	86
INVESTIGATING CIVILIAN CASUALTIES IN ARMED CONFLICT: COMPARING U.S. MILITARY INVESTIGATIONS WITH ALTERNATIVES UNDER INTERNATIONAL HUMANITARIAN AND HUMAN RIGHTS LAW Commander Sylvaine Wong, JAGC, USN	111

Book Review

FORCES OF FORTUNE: THE RISE OF THE NEW MUSLIM MIDDLE CLASS AND WHAT IT WILL MEAN FOR OUR WORLD Major Alex M. Straub, ARNG	168
THE GOOD SOLDIERS Major Timothy W. Thomas, USA	175

STUXNET AND ARTICLE 2(4)'S PROHIBITION AGAINST THE USE OF FORCE: CUSTOMARY LAW AND POTENTIAL MODELS

Lieutenant Andrew Moore, JAGC, USN*

I. Introduction

The customary interpretation of the United Nations (U.N.) Charter's Article 2(4) prohibition against the use of force is ill-suited for coercive uses of the cyber instrument, such as the Stuxnet cyberattack. Since its drafting, the U.N. Charter has been the relevant set of international conflict management principles—specifically Article 2(4). Drafted in the wake of World War II's destruction, the customary interpretation of Article 2(4), and the state practice surrounding its prohibition against force, has focused on restricting the use of the military instrument. Article 2(4)'s textual ambiguity and flexibility has allowed it to remain relevant in regulating weapons based in the physical domain. Unforeseen at the time of the U.N. Charter's drafting, the cyber domain and its use as a means of inter-state coercion pose a challenge to Article 2(4)'s prevailing instrument-based interpretation of force.¹

In order to remain relevant, the customary interpretation of Article 2(4)'s prohibition against force must evolve to address coercive uses of the cyber instrument by nation-states. The Stuxnet malware demonstrates the lacunae between the accepted “use of force” analysis for the use of the military instrument and the cyber instrument under Article 2(4). The destruction caused to the Iranian nuclear complex demonstrates that Stuxnet should be considered a use of force prohibited by Article 2(4), and, possibly, equivalent to an armed attack. In a six-month period from late 2009 until 2010, a malicious software, or malware, named Stuxnet infiltrated and attacked the control systems at Iran's largest nuclear fuel

* Lieutenant, Judge Advocate General's Corps, United States Navy. B.A. University of Minnesota, 2003; J.D., Georgetown University Law Center, 2011. The views expressed in this document are those of the author and do not represent the views of the Department of Defense or the Department of the Navy.

¹ The instrument-based interpretation of force categorizes actions taken by a nation-state against another nation-state based on the means used. See Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. OF TRANSNAT'L L. 885, 904 (1999) (stating that the determination of whether or not the standard has been breached depends on the type of the coercive instrument—diplomatic, economic, or military—selected to attain the national objectives in question).

enrichment facility, Natanz. During that time, Stuxnet destroyed ten percent of the centrifuges the facility.² Despite the physical destruction, this act of coercion is outside of the ambit of Article 2(4) under the customary instrument-based interpretation.

Stuxnet provided an opportunity to evolve the customary interpretation of Article 2(4)'s prohibition against the use of force to include the coercive use of the cyber instrument.³ This paper will address the customary interpretation of force prohibited by Article 2(4), models for applying Article 2(4) to the use of the cyber instrument, and whether the Stuxnet malware attack on the Iranian nuclear complex reaches the level of a "use of force" in violation of Article 2(4) under these models. To focus on the legal issues of the use of the cyber instrument as a method of interstate coercion, the scope of Iran's response to Stuxnet is not addressed.

The following assumptions are used to focus the paper on the challenge of applying Article 2(4) to the coercive use of the cyber instrument,⁴ as evidenced by Stuxnet. First, it is assumed that a nation-state is responsible for deploying Stuxnet.⁵ Second, the analysis assumes that attributing Stuxnet to the responsible state has occurred.⁶ Third, the deployment of Stuxnet is assumed to have occurred

² See William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iranian Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, at A1.

³ State practice and *opinio juris* have begun to evolve the interpretation of Article 2(4) to apply to uses of the cyber instrument. See The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* 9 (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter White House Cyber Policy]; Harold Honhgu Koh, Legal Advisor of the Dep't of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (Sep. 18, 2012), *available at*

<http://www.state.gov/s/l/releases/remarks/197924.htm> [hereinafter Koh speech]; INTERNATIONAL GROUP OF EXPERTS, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael Schmitt ed., 2013) [hereinafter TALLINN MANUAL]. The Tallinn Manual consists of "rules" adopted unanimously by an international group of legal and technical experts that are meant to reflect customary international law, accompanied by "commentary" that outlines their legal basis and highlights any differences of opinion among the Experts as to their interpretation in the cyber context. Michael Schmitt served as the project's director. Prof. Schmitt is one of the foremost writers on the application of the Law of Armed Conflict to the actions taken within the cyber domain.

⁴ This term refers to any hostile act in the virtual reality of cyberspace that has manifestations in the physical world, such as a cyberattack. The National Research Council (NRC) Report *infra* has distinguished cyberattacks, or offensive cyber operations, from other cyber activity as one that has a destructive payload.

⁵ The author recognizes attribution may be the most challenging, if not effectively impossible, technical aspect of analyzing the use of the cyber instrument, but this technical challenge does not change the use of force analysis.

⁶ To date, no country has publically taken responsibility for Stuxnet. See, e.g., *Iran: Computer Worm Could Have Caused Huge Damage*, ASSOC. PRESS, Apr. 17, 2011, *available at* <http://phys.org/news/2011-04-iran-worm-huge.html> (citing Iranian officials who have determined that the United States and Israel were responsible); David E. Sanger, *Obama Order Sped Up Wave of*

outside of a U.N. authorized use of force, and was not conducted in self-defense under Article 51. Fourth, the state responsible for deploying Stuxnet is assumed to have intended to cause physical damage in the target state, specifically to critical infrastructure, such as telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services.⁷

Given these assumptions, the paper will examine Stuxnet and the analytical models for determining whether it is or should be considered a use of force under Article 2(4). Part II is an overview of Stuxnet's attack method, target, and effects. Part III examines the customary interpretation of which forms of coercion constitute a prohibited use of force under Article 2(4) and customary international law. Part IV outlines three proposed analytical models for applying Article 2(4) to coercive uses of the cyber instrument between states. Part V examines whether Stuxnet is a use of force in violation of Article 2(4) under each of the three models. Part VI is the conclusion, which stresses that the interpretation of Article 2(4)'s prohibition against force should evolve to include coercive uses of the cyber instrument that have destructive effects in the physical world such as Stuxnet.

II. Stuxnet

In June 2010, the discovery of a malware that targeted control systems at the Iranian nuclear facility Natanz was first publicly reported.⁸ Malware is malicious software that interferes with normal computer and Internet-based application functions.⁹ The malware's name, Stuxnet, is derived from keywords buried in its code.¹⁰ Although malware has existed since the inception of computer networks, Stuxnet has been recognized as a *magnum opus* in terms of concept of its operation, elegance of its design, and effectiveness of its code.¹¹ This sophistication

Cyberattacks Against Iran, N.Y. TIMES, Jun. 1, 2012, at A1 (citing unnamed current and former American, European and Israeli officials who confirmed U.S. and Israeli involvement in launching Stuxnet). See also DAVID E. SANGER, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (2012); David Kushner, *The Real Story of Stuxnet*, IEEE Spectrum, Feb. 26, 2013, available at <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

⁷ See Exec. Order No. 13,010, 61 Fed Reg. 37,347 (1996) (defining which systems and infrastructure are critical, sensitive, and vital).

⁸ Brian Krebs, *Experts Warn of a New Windows Shortcut Flaw*, KREBS ON SECURITY (Jul. 18, 2010), <http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/>.

⁹ Troy Nash, U. S. DEPARTMENT OF HOMELAND SECURITY, AN UNDIRECTED ATTACK AGAINST CRITICAL INFRASTRUCTURE (2005), available at https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/CaseStudy-002.pdf.

¹⁰ *A Worm in the Centrifuge*, THE ECONOMIST, Sept. 30, 2010, available at <http://www.economist.com/node/17147818>.

¹¹ Greg Keizer, *Is Stuxnet the 'Best' Malware Ever?*, COMPUTERWORLD, Sept. 16, 2010, available at http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_.

may be an indication that it was the result of a state-sponsored project to hamper Iran's pursuit of nuclear technology.¹²

There are two classes of targeted malware attacks: attacks targeting a specific company or organization, and attacks targeting specific software or information technology (IT) infrastructure.¹³ Stuxnet falls in the second class of malware attacks targeting specific software and IT infrastructure.¹⁴ Moreover, Stuxnet was more precise than a targeted attack-- it was designed and executed as a directed attack.¹⁵ Whereas a targeted attack is one that has been aimed at a specific user, company or organization, a directed attack is designed to attack a single system within a specific organization.¹⁶

Stuxnet targeted industrial software and equipment or Supervisory Control and Data Acquisition (SCADA) systems.¹⁷ SCADA systems monitor and control industrial, infrastructure, or facility-based processes.¹⁸ SCADA systems are usually built with proprietary software, and are often not connected to the Internet. A malware's payload is the data or destructive effect that is transmitted to the target. Stuxnet's payload was designed to target and deliver its payload only to the specific SCADA systems used at the Natanz uranium enrichment facility in Iran.¹⁹

Stuxnet was a well-designed attack²⁰ and had a promiscuous propagation, or aggressive growth pattern with limited controls.²¹ However, once Stuxnet came

¹² *Id.*

¹³ See Aleksandr Matrosov, *Stuxnet Under the Microscope*, ESET 5 (last visited May 27, 2015), http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

¹⁴ *Id.*

¹⁵ See Ralph Langner, *Cracking Stuxnet, a 21st Century Cyber Weapon*, TED, (Mar. 2011), *available at* http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html?awesm=on.ted.com_Langner&utm_content=awesm-publisher&utm_medium=on.ted.com-static&utm_source=langner.com [hereinafter Langner speech].

¹⁶ See Matrosov, *supra* note 13, at 5.

¹⁷ See, e.g., Nicolas Falliere, Liam O. Murchu, & Eric Chien, *W32.Stuxnet Dossier*, v. 1.4, SYMANTEC (Feb. 2011),

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [hereinafter Symantec]; *Iran's Nuclear Agency Trying to Stop Computer Worm*, ASSOC. PRESS, Sep 25, 2010, *available at* <http://www.independent.co.uk/news/world/middle-east/irans-nuclear-agency-trying-to-stop-computer-worm-2089447.html>.

¹⁸ *SCADA*, TECH-FAQ, (last visited May 28, 2015), <http://www.tech-faq.com/scada.html>. Although the potential for collateral damage of releasing malware targeted at SCADA systems into the open became a reality, the code only deployed the destructive payload on a specific target).

¹⁹ See Ralph Langner, *Year-end Roundup*, LANGNER (Dec. 31, 2010), <http://www.langner.com/en/2010/12/31/year-end-roundup/>; Christopher Williams, *Cyberattack on Iran 'was carried out by Western powers and Israel'*, THE TELEGRAPH, Jan. 21, 2011, *available at* <http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html>.

²⁰ It is unclear at what point Iran completely eliminated or even stopped Stuxnet. See Thomas Erdbrink and Joby Warrick, *Iran: Country Under Attack by Second Computer Virus*, WASH. POST,

into contact with the target system, it automatically deployed its attack.²² Stuxnet was able to surreptitiously remain undetected because it used digital signatures to gain access privileges and maintain anonymity in a secured network.²³ The malware used the highest level of privileges available in order to take any action it wanted on the infiltrated computer.²⁴ In instances when Stuxnet did not have the requisite privileges, it used one of four self-launching, zero-day attacks, which exploit vulnerabilities in software that are unknown to others including the software developer.²⁵ These zero-day attacks were used to install undetected, malicious programs onto the system and gain access to networks.²⁶

Stuxnet's infiltration plan consisted of two steps, each with its own payload: one exploitative and the other destructive.²⁷ The first step, called a dropper, issued to compromise a laptop computer that is running regular Microsoft Windows to configure the SCADA systems at Natanz.²⁸ Second, after the dropper has gained control of the laptop, it exploits the laptop as an entry point into the SCADA system. During this second step, the malware searches for a specific configuration only found in the SCADA system being utilized at Natanz.²⁹ If Stuxnet does not find the specific configuration, it does nothing. If it does recognize the configuration, then it begins the next phase of the attack by launching the destructive payload.³⁰

After Stuxnet infiltrated the targeted SCADA system at Natanz, it worked at the same target from two different avenues of approach while manipulating data being sent to the control room and safety systems.³¹ One approach took control of the centrifuge systems and began to spin them slower and faster in order to crack and destroy them.³² The second approach took control of the nuclear fuel cascade process, and began to manipulate the process causing damage to the system.³³ In addition to attacks from two approaches, Stuxnet was designed to deceive the

Apr. 25, 2011, available at http://www.washingtonpost.com/world/iran-country-under-attack-by-second-computer-virus/2011/04/25/AFudKBjE_story.html.

²¹ See Matrosov, *supra* note 13, at 10.

²² See *Stuxnet: Targeting Iran's Nuclear Programme*, INT'L INST. FOR STRATEGIC STUDIES (Feb. 2011), <http://www.iiss.org/publications/strategic-comments/past-issues/volume-17-2011/february/stuxnet-targeting-irans-nuclear-programme/> [hereinafter IISS].

²³ See Matrosov, *supra* note 13, at 7.

²⁴ See Symantec, *supra* note 17.

²⁵ See Matrosov, *supra* note 13, at 7; Symantec, *supra* note 17; see also Keizer, *supra* note 12 (according to O Muchu, the four zero-day attacks are unprecedented for a single piece of malware).

²⁶ See Symantec, *supra* note 17.

²⁷ See Langner speech, *supra* note 15; IISS *supra* note 22.

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

³¹ See Symantec, *supra* note 17.

³² See IISS, *supra* note 22.

³³ *Id.*

engineers in the control room by sending false data that is consistent with regular centrifuge and cascade processes.³⁴ Further, Stuxnet malware compromised digital safety systems preventing the automated systems from halting an unsafe process.³⁵

Stuxnet was able to accomplish what U.N. economic sanctions have not been able to do—hamper the Iranian nuclear program. Stuxnet had a detrimental effect on the Iranian nuclear complex, specifically the Natanz fuel enrichment plant.³⁶ One report indicates that Stuxnet has set the Iranian nuclear program back by as much as two years.³⁷ According to reports by the International Atomic Energy Agency and other nuclear watchdogs, Iran dismantled and then replaced more than ten percent of the 9,000 centrifuges at the Natanz facility during a six month period from late 2009 until the spring of 2010, including all 984 centrifuges in six cascades.³⁸ The destruction of the centrifuges may not appear significant since Iran was able to increase its amount of low enriched uranium (LEU) during the time of the attack, but Stuxnet was able to delay Iran from increasing the number of enriching centrifuges.³⁹ Although it appears Iran's LEU production has recovered, it is unclear if Iranian leaders' confidence or Iranian nuclear facilities' computer systems have recovered from Stuxnet.⁴⁰

Stuxnet has significant implications beyond the direct physical effects on the speculated target, Natanz. Stuxnet's complexity and sophistication indicate nation-state sponsorship of a well-coordinated, well-resourced, and highly-skilled team effort in creating, testing, and monitoring Stuxnet.⁴¹ As the Battle of Agincourt and the bombing of Hiroshima were examples of new means of violence and destruction,⁴² Stuxnet may signal an intensification of the coercive use of the cyber instrument between nation-states. Worse, the physical effects and legal

³⁴ See Langner, *supra* note 19.

³⁵ See Langner Speech, *supra* note 15.

³⁶ See Joby Warrick, *Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack*, WASH. POST, Feb. 16, 2011, available at <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html>.

³⁷ See IISS, *supra* note 22 (citing IT security analyst and Stuxnet expert Ralph Langner).

³⁸ See *id.*

³⁹ IISS, *supra* note 22 (the totality of Stuxnet's effects on Natanz and the Iranian nuclear complex is unclear).

⁴⁰ See IISS, *supra* note 23 (Iranian President Mahmoud Ahmadinejad admitted that Iran had been the target of a cyberattack, which he blamed on the West); Thomas Erdbrink & Joby Warrick, *Iran: Country Under Attack by Second Computer Virus*, WASH. POST, Apr. 25, 2011, available at http://www.washingtonpost.com/world/iran-country-under-attack-by-second-computer-virus/2011/04/25/AFudkBjE_story.html.

⁴¹ See, e.g., Langner, *supra* note 19; Keizer, *supra* note 11.

⁴² The Battle of Agincourt in 1415 is noted as one of the first battles to experience extensive use of the English long-bow, which led to an extremely lopsided victory for the outnumbered English forces that left almost 10,000 French soldiers dead. See, e.g., Hannah Ellis Peterson, *Ten Reason Why the French Lost*, THE TELEGRAPH, Jul. 20, 2011 available at <http://www.telegraph.co.uk/news/8648068/Battle-of-Agincourt-ten-reasons-why-the-French-lost.html>.

implications of Stuxnet are a harbinger of a form of international coercion unforeseen by Charter drafters and unsettled under prevailing international law.

III. International Law: *Jus Ad Bellum* and prohibited ‘Use of Force’ under Article 2(4) of the United Nations Charter

In order to analyze inter-state coercive uses of the cyber instrument such as Stuxnet, it is imperative to understand the prevailing legal framework, specifically the international law of armed conflict (LOAC). One of the questions LOAC addresses is “when is it legal for one nation-state to use force against another?” This body of law is known as *Jus Ad Bellum*.⁴³ Until the advent of the U.N. and its Charter, unilateral use of force in inter-state relations was lawful.⁴⁴ Now, *Jus Ad Bellum* is governed primarily by the U.N. Charter, interpretations of the U.N. Charter, other international conventions, and customary international law that has been formed by *opinio juris* and state practice.⁴⁵

The U.N. Charter attempted to codify how states could engage with each other. The Charter prohibits the unilateral use of force for any reason except self-defense.⁴⁶ However, neither the U.N. Charter nor customary international law offers a clear definition for what constitutes a prohibited use of force by a state. Article 2(4) of the U.N. Charter is the most relevant section in determining a state’s ability to use force unilaterally outside of the self-defense context, prohibiting states from the unilateral threat or use of force.⁴⁷ Although on its face these provisions appear plain, as discussed below, the interpretation and application of Article 2(4) in inter-state relations are uncertain, specifically the definition of a “use of force.”

Under Article 2(4), U.N. Member states are prohibited from “the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”⁴⁸ The Charter allows for the use of force in only two situations: where it is authorized by

⁴³ See David E. Graham, *Cyber Threats and the Law of War*, 4 J. OF NAT. SEC. LAW & POL. 87 (2010) (referring to *Jus Ad Bellum* as a set of conflict management norms and procedures as opposed to a set of laws) (*Jus in bello* is not addressed in this paper).

⁴⁴ See W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION 39-40 (Yale Univ. Press 1992).

⁴⁵ See, e.g., Commander Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During a Fundamental Change in the Nature of Warfare*, 60 NAVAL L. REV. 1 (2010); NATIONAL RESEARCH COUNCIL COMMITTEE ON OFFENSIVE INFORMATION WARFARE, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens, Kenneth W. Dam, & Herbert S. Lin, eds., 2009) (hereinafter NRC REPORT).

⁴⁶ Even then the U.N. Charter regulates the process of self-defense. See U.N. Charter art. 51.

⁴⁷ See U.N. Charter art. 51.

⁴⁸ U.N. Charter art. 2, ¶ 4.

the U.N. Security Council under Chapter VII and when it is done in self-defense to an armed attack under Article 51.⁴⁹

Drafted in the wake of World War II's destruction, Article 2(4) and state practice surrounding its prohibition against force focused on restricting the use of the military instrument. According to Reisman and Baker:

[b]oth the Charter, and its reformulations by the Assembly and customary conceptions of international law with regard to the use of the military instrument rested on a set of inherited assumptions about how military conflict is conducted: conflict is territorial, between organized communities Changes in military technology and political dynamics made many of the key assumptions underlying the basic rules about when and how to use force obsolete.⁵⁰

Article 2(4) does not define what constitutes a "use of force",⁵¹ however, other U.N. provisions aid in determining what activities may constitute a use of force. Article 41 lists measures which are not uses of force, including complete or partial disruption of economic relations of rail, sea, air, telephonic, and other means of communication.⁵² Article 42 gives additional specific uses of force including "blockades and other operations by armed forces."⁵³

Article 2(4) is both direct and ambiguous in its prohibition of the use of force by states.⁵⁴ The Vienna Convention on the Law of Treaties outlines that international instruments should be interpreted "in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and scope."⁵⁵ A face value reading of Article 2(4) prohibits states from threatening or using force against other states.⁵⁶ But, a face value reading of the article fails to provide an interpretation that is applicable without context. This ambiguity enables the U.N., regional organizations, and individual states more flexibility in applying the provision's language to situations as they arise. As Prof.

⁴⁹ See U.N. Charter arts. 42 & 51.

⁵⁰ Reisman & Baker, *supra* note 44, at 41.

⁵¹ See, e.g., Oscar Schachter, *In Defense of International Rules on the Use of Force*, 53 U. CHI. L. REV. 113, 127 (1986); YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 18 (2d ed. 1994); W. Michael Reisman, *Article 2(4): The Use of Force in Contemporary International Law*, 78-79 AM. SOC. INT'L L. PROC. 74, 79-84 (1984-85).

⁵² U.N. Charter art. 41.

⁵³ U.N. Charter art. 42.

⁵⁴ Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 426-30 (2011).

⁵⁵ Vienna Convention on the Law of Treaties, art. 31(1), May 23, 1969, 1155 U.N.T.S. 331 (1969).

⁵⁶ See, Graham, *supra* note 43.

Michael Schmitt states, “because the Charter is the constitutive instrument of an international organization, flexibility in interpretive spirit is apropos.”⁵⁷ This flexibility does not mean “that the rules lack any content.”⁵⁸

International legal scholars have debated the meaning of Article 2(4) and the term “use of force.”⁵⁹ Historically, a “use of force” has been defined in terms of the instrument used, including ‘armed force’ within the prohibition, but excluding economic and political coercion.⁶⁰ The customary interpretation of Article 2(4) determines a “use of force” using an instrument-based analysis. The U.S. and its international allies view Article 2(4) as applying to armed attacks of one state against another.⁶¹ A plain reading of Article 2(4) and other structural aspects of the Charter support this view.⁶² The purpose of the Charter is “to save succeeding generations from the scourge of war,” but does not ban other forms of coercion.⁶³ Further, the *travaux préparatoires* indicated that the drafters did not intend to extend the prohibition on force to economic or political pressures.⁶⁴

U.N. and other international pronouncements militate towards an instrument-based analysis in defining a use of force. The U.N. General Assembly’s definition of aggression requires the use of an armed force against another state, and provides a non-exhaustive list of acts that qualify as acts of aggression.⁶⁵

⁵⁷ Schmitt, *supra* note 1.

⁵⁸ Schacter, *supra* note 51 at 121; Dinstein, *supra* note 51.

⁵⁹ See, e.g., *id.*

⁶⁰ Schmitt, *supra* note 1, at 919.

⁶¹ See NRC REPORT, *supra* note 45, at 253 (“Traditional LOAC emphasizes death or physical injury to people and destruction of physical property as criteria for the definitions of ‘use of force’ and ‘armed attack.’”); Albrecht Randelzhofer, *Art. 2(4)*, in *THE CHARTER OF THE UNITED NATIONS: A COMMENTARY*, 112, 117 (2d ed., Bruno Simma, ed., 2002) (noting that art. 2(4) is, “according to the correct and prevailing view, limited to armed force.”).

⁶² Waxman, *supra* note 54, at 428 (“[T]he Charter’s preamble sets out the goal that ‘armed force . . . not be used save in the common interest.’ Similarly, Articles 41 and 42 authorize, respectively, the Security Council to take actions not involving armed force and, should those measures be inadequate, to escalate to armed force. Moreover, Article 51 speaks of self-defense against ‘armed’ attacks. There are textual counter-arguments, such as that Article 51’s more specific limit to ‘armed attacks’ suggests that drafters envisioned prohibited ‘force’ as a broader category not limited to particular methods. However, the discussions of means throughout the Charter and the document’s negotiating history strongly suggest the drafters’ intention to regulate armed force differently and more strictly than other coercive instruments.” (ellipsis and emphasis in original) (footnotes omitted)).

⁶³ See Marco Roscini, *World Wide Warfare—Jus ad Bellum and the Use of Cyber Force*, 14 MAX PLANCK Y.B. UNITED NATIONS L. 85, 105 (2010).

⁶⁴ See *id.*; see also Charter of the Organization of American States art. 18, Apr. 30, 1948, T.I.A.S. No. 2361, 119 U.N.T.S. 3 (“No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. The foregoing principle prohibits not only armed force but also any other form of interference or attempted threat against the personality of the State or against its political, economic, and cultural elements.”) (distinguishing armed force from economic and political force).

⁶⁵ Definition of Aggression, G.A. Res. 3314 (XXIX), arts. 1, 3, 4, U.N. Doc. A/3314 (Dec. 14, 1974).

Article 49 of Additional Protocol I of the Geneva Conventions defines attacks and scope of application to include “acts of violence against the adversary,” and specifies that it applies to “any land, air, or sea” warfare.⁶⁶

As demonstrated by post-Charter practice, use of force analysis places coercive acts on a continuum.⁶⁷ Along the coercive acts continuum, economic and diplomatic acts lie at one extreme and armed attacks lie at the other. Economic and diplomatic acts are not uses of force under the customary interpretation of Article 2(4). Armed attacks are uses of force, and such attacks afford nation-states the right to use force in self-defense.⁶⁸ In between these extremes is a “use of force” threshold.

Advocates of the instrument-based analysis categorize a use of force into one of three levels: aggression, self-defense, and sanctions authorized or ordered by the U.N. Security Council.⁶⁹ With these categories, Article 2(4)'s prohibition against a use of force could be violated only by uses of the military instrument. However, these categories created by practice may fail to recognize other prohibited uses of force that have evolved since the drafting of the Charter.⁷⁰

One example of the possible gaps caused by a strict adherence to the instrument-based analysis is found by examining the disparate treatment under international law for economic sanctions and blockades.⁷¹ Whereas an instrument-based analysis would classify a blockade as a use of force, an effects-based analysis would categorize both means as uses of force if they had similar effects on the target country.

The Declaration of Friendly Relations supports a more expansive reading of the text of Article 2(4) prohibiting more than armed force and adopting a more effects-based analysis. Such a reading would view Article 2(4) as a prohibition

⁶⁶ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 49, Jun. 8, 1977, 1125 U.N.T.S. 3.

⁶⁷ See Huntley, *supra* note 45, at 18 (positing “the use of force analysis as taking place on a continuum, where armed attacks, the existence of which gives rise to a right to use force in self-defense, lie at one extreme, and where coercive but permissible acts such as economic coercion...lie at the opposite end of the continuum.”).

⁶⁸ See Huntley, *supra* note 45, at 18. Schmitt refers to this as a “community values threat continuum.” *Supra* note 1 at 912.

⁶⁹ See TALLIN MANUAL, *supra* note 3, R. 11, 13, 18; Tom J. Farer, *Political and Economic Coercion in Contemporary International Law*, 79 AM J. INT'L L. 405, 408 (1985).

⁷⁰ See Schmitt, *supra* note 1.

⁷¹ See Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 61 (2010), available at http://www.jnslp.com/read/vol4no1/06_Lin_vol4no1.asp at 80 (citing Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 84-85 (2001)).

against coercion.⁷² Mirroring the language of Article 2(4), the Declaration of Friendly Relations prohibits states from using any means of coercion to intervene in the affairs of another state, directly or indirectly.⁷³ Under this analysis, the use of other non-military instruments of national power could rise to the level of a use of force.⁷⁴

The International Court of Justice (ICJ) did not directly adopt an instrument-based analysis for a violation of the Article 2(4) prohibition against the use of force in its advisory opinion on the *Threat or Use of Nuclear Weapons*.⁷⁵ The ICJ found that Article 2(4) and other provisions related to the use of force “do not refer to specific weapons.”⁷⁶ Further, the ICJ stated, “[t]hey apply to any use of force, regardless of the weapons employed ... The Charter neither expressly prohibits, nor permits, the use of any specific weapon.”⁷⁷

In *Nicaragua v. United States*, the ICJ attempted to clarify what is a use of force.⁷⁸ In its analysis, the ICJ looked to the scope and magnitude of the effects on the victim state. The ICJ held the U.S.’s laying of mines in Nicaraguan territorial waters was a use of force.⁷⁹ According to the ICJ, Article 2(4)’s prohibition against the threat or use of force mirrored customary international law’s same prohibition.⁸⁰ Further, the ICJ analyzed varying levels of U.S. activities in support of the *contras*.⁸¹ The ICJ’s examination included the U.S. provision of funds, the U.S. provision of extensive logistical military support, and U.S. participation in the planning, direction, and execution of a series of attacks on Nicaraguan facilities.⁸² The ICJ found the provision of funds was a violation of the principle of non-intervention, but did not violate the prohibition against the use of force.⁸³ However,

⁷² See Waxman, *supra* note 54, at 428-29; DINSTEIN, *supra* note 51, at 18.

⁷³ See G.A. Res. 2625 (XXV), U.N. Doc. A/8082, at 122 (Oct. 24, 1970) (General Assembly Resolutions are not binding towards member states).

⁷⁴ See generally Farer, *supra* note 69 (stating that it is highly unlikely that requisite conditions could be met for acts of political and economic coercion to rise to the level of aggression comparable to military aggression); JULIUS STONE, *CONFLICT THROUGH CONSENSUS* (1977) (stating that the consensus definition of aggression adopted by the U.N. prohibits infringements against nation-state’s sovereignty in addition to its territorial integrity and political independence; thus, evidences an evolution towards a broader definition of what coercive acts are prohibited).

⁷⁵ See *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ¶ 39 (July 8, 1996), available at <http://www.icj-cij.org/docket/files/95/7495.pdf>.

⁷⁶ See *id.*

⁷⁷ *Id.*

⁷⁸ See *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. 14 (June 27), available at <http://www.icj-cij.org/docket/files/70/6503.pdf> [hereinafter *Nicar. v. U.S.*].

⁷⁹ *Id.*

⁸⁰ *Id.* ¶ 147.

⁸¹ *Id.* ¶ 228.

⁸² *Id.* ¶¶ 81-86.

⁸³ *Id.* ¶ 228.

the U.S. military's logistical support and involvement in the attacks on Nicaraguan facilities violated the prohibition against the use of force, but did not rise to the level of an armed attack.⁸⁴

Although the ICJ adopted a more expansive view of the prohibition against force, states have repeatedly used economic and other forms of coercion without legal challenge.⁸⁵ Expanding the definition for a "use of force" to include economic and political coercion has been criticized and not been reflected in state practice.⁸⁶ Thus, the post-Charter practice indicates that the instrument-based analysis of a use of force prevails.⁸⁷ Although military forces were involved in Nicaragua, the ICJ suggested that other forms of coercion should be deemed as prohibited uses of force under Article 2(4).⁸⁸

Despite the ICJ's expanded interpretation of what constitutes a prohibited use of force, the customary instrument-based analysis is effective because of the congruence between the instrument used and its physical effects.⁸⁹ Although use of force analysis focuses on the instrument used, it is the physically harmful and damaging effects, not the means of the instruments, that render them counter to the purposes of the U.N. Charter and international law.⁹⁰

The instrument-based interpretation of Article 2(4) set a threshold on the continuum of coercion where acts are categorized as force. The ICJ's decisions expanded the zone of force by pushing that threshold away from armed attack and towards diplomatic and economic acts. The ICJ's expansion of the definition of force beyond the ambit of an instrument-based approach creates uncertainty as to where exactly the use of force threshold falls on the coercion continuum until state practice and other means of norm formation are established.

⁸⁴ *Id.* ¶ 195.

⁸⁵ See Farer, *supra* note 69.

⁸⁶ See generally IAN BROWNIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES (1963) ("[s]ubversion and economic pressure will present really serious dangers to a state only in exceptional circumstances and it is not being realistic to deprive the law of its general efficacy by demanding a new legal regime based on vague criteria solely to deal with rare circumstances. In any case, states need not submit to subversion and economic pressure, but may take all possible counter-measures in their territory.").

⁸⁷ See, e.g., Schmitt, *supra* note 1, at 15.

⁸⁸ See Sean D. Murphy, *Protean Jus Ad Bellum*, 27 BERKELEY J. INT'L L. 22, 30 (2009) ("More interesting was the Court's conclusion that certain acts in violation of Article 2(4) might not rise to the threshold of being an 'armed attack' for purposes of Article 51, and therefore could not be responded to through the exercise of self-defense. This lack of symmetry between Articles 2(4) and 51 is well-grounded textually in the Charter, but it also rather unsatisfactorily invites coercive behavior that operates below the radar of 'armed attack,' and hence has been criticized."); Schmitt, *supra* note 1, at 923.

⁸⁹ See Schmitt, *supra* note 1, at 922.

⁹⁰ See BROWNIE, *supra* note 86, at 362.

Although Article 2(4) is the primary basis for governing acts of coercion and prohibiting force, a similar prohibition on force is found under customary international law and *jus cogens*.⁹¹ In *Nicaragua*, the ICJ did not base its decision on Article 2(4), but on customary international law. The ICJ acknowledged that the two interpretations, while similar, do not coincide.⁹² The interpretation of Article 2(4) can evolve based on state consent and contextual interpretation.⁹³ Customary international law cannot evolve unless there is state practice and *opinio juris*.⁹⁴ Thus, with state consent and contextual interpretation, an act of coercion could expand the interpretation of what level of coercion is prohibited as force under Article 2(4), and this interpretation can begin the formation of a new norm of customary law. Beginning with Article 2(4), an evolution of the interpretation of force is important to the international system because of the advent of new forms of coercion.⁹⁵

The customary interpretations of what constitutes a use of force should progress as technology advances bringing new instruments of national power, new domains for battle space, and new methods of coercion. As identified by Reisman, categories themselves are not determinative, but each threat or use of force should be evaluated based on the context in which it occurs.⁹⁶ Coercive uses of the cyber instrument demand a more evolved use of force analysis.⁹⁷

IV. Applying Article 2(4) to Use of the Cyber Instrument

The question of whether a coercive use of the cyber instrument constitutes a use of force or an armed attack is significant in determining what responses would be legitimate under international law.⁹⁸ With a destructive cyberattack on critical infrastructure, a coercive use of the cyber instrument could have effects in the physical world. The physical effects of coercive uses of the cyber instrument may be analogous, if not identical, to the physical effects of coercive uses of the military instrument. However, even without the problem of attributing cyberattacks to responsible states, coercive uses of the cyber instrument are outside the ambit of Article 2(4)'s prohibition against force under the customary interpretation. Similar

⁹¹ See Schmitt, *supra* note 1, at 922 (citing Report of the International Law Commission, 18th Sess., 1966 (II) I.L.C.Y.B. 247, and 1968 I.C.J. 4, 100).

⁹² See *id.* at 903 (citing *Nicar. v. U.S.*).

⁹³ See *id.* at 903.

⁹⁴ See *id.* at 904.

⁹⁵ See *id.* at 899.

⁹⁶ See Reisman, *supra* note 51, at 282; TALLINN MANUAL, *supra* note 3.

⁹⁷ See, e.g., TALLINN MANUAL, *supra* note 3; Schmitt, *infra* note 100; Schmitt, *supra* note 1; Waxman, *supra* note 54.

⁹⁸ See Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense*, 38 STAN. J. INT'L L., 207, 208 (2002); WALTER GARY SHARP, CYBERSPACE AND THE USE OF FORCE 7, 28 (1999).

to the application of Article 2(4) to the use of non-kinetic armed force,⁹⁹ the context of the use of the cyber instrument analysis focuses on the effects of the act. The application of Article 2(4) to the use of the cyber instrument would be an evolution and expansion of its scope, but not an alteration of its spirit.¹⁰⁰ In order for Article 2(4) to remain as the relevant regulation for inter-state coercion, the analysis below assumes an evolution of the customary interpretation of Article 2(4) to include the use of the cyber instrument. Three potential analytical models are presented for examining whether coercive uses of the cyber instrument violate Article 2(4).

Unlike uses of the military instrument that are easy to attribute to the responsible state, coercive uses of the cyber instrument are problematic, if not impossible, to attribute to the responsible state because of the nature of the instrument.¹⁰¹ With the problem of attribution, states that have and continue to use the cyber instrument as a tool in inter-state relations have limited incentive to support an evolution of the interpretation. By using the cyber instrument, states would be in violation of the new interpretation. Conversely, by not using the cyber instrument, states would be limiting themselves from using their full complement of tools for inter-state relations.

Even with attribution, states could employ the cyber instrument as a means of coercion causing harm to other states without violating international law unless the customary interpretation of Article 2(4) evolves; such a situation would be disruptive to international order and damaging to the relevancy of Article 2(4). Stuxnet may be the most elegant malware devised, but it is not the only example of a coercive use of the cyber instrument.¹⁰² As Stuxnet demonstrates, the use or threat

⁹⁹ Such as international prohibitions on chemical and biological weapons. See Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, Apr. 10, 1972, 26 U.S.T.S. 583, 1015 U.N.T.S. 163; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, adopted Sept. 3, 1992, 1974 U.N.T.S. 45.

¹⁰⁰ See Michael Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L. J. 13, 36 (2012) (highlighting how the Koh speech, and the Tallinn Manual *supra* note 3, demonstrate the evolving interpretation and application of Article 2(4) to state conduct in cyberspace); see also White House Cyber Policy, *supra* note 3 ("The development of norms for state conduct in cyberspace does not require a reinvention of customary international law Long-standing international norms guiding state behavior . . . also apply in cyberspace."); John Richardson, *Stuxnet as Cyberwarfare: Applying Law of War to Virtual Battlefield*, 29 J. MARSHALL J. COMPUTER & INFO. L. 1 (2011); Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842 (2012); see generally, MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW (2014).

¹⁰¹ See Schmitt, *supra* note 100, at 17 (that "it became clear during the [Tallinn] project's proceedings that interpretation of international law norms in the cyber context can be challenging.")

¹⁰² See, e.g., Dan Elliot, *Retired General: US Vulnerable to Cyberattacks*, ASSOC. PRESS, Apr. 11, 2011, available at <http://www.businessweek.com/ap/financialnews/D9MHLMCG0.html> (quoting former U.S. Joint Chiefs of Staff chairman General Peter Pace, USMC (Ret) that the United States "has employed cyberattacks in the past"); John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 12, 2008,

of use of the cyber instrument by one state can have deleterious effects on another state's critical infrastructure. Under accepted international law, it is unclear what response options a targeted state may have to remedy the situation.¹⁰³ Given the recent coercive uses of cyber instrument by permanent members of the U.N. Security Council, it is unlikely that the Council will take any action under Article 39.¹⁰⁴ As uses of the cyber instrument increase in frequency as a means of interstate coercion, failure to evolve the current instrument-based definition of force could be damaging to the relevancy of Article 2(4) and disruptive to the stability of international order because states will use, or threaten to use, harmful coercive means without violating international law.¹⁰⁵ Although lawful, such coercive uses of the cyber instrument could trigger responses that would be in violation of Article 2(4) by targeted states.

Coercive use of the cyber instrument presents a challenge to the customary coercion continuum analysis because the instrument used is not a traditional military force, and both the direct and indirect consequences of its use can vary in severity. Despite these difficulties, recent state practice has demonstrated that the cyber domain is viewed as another platform for interstate coercion; essentially cyberspace is a new battle space. As Jensen observed, "it is unreasonable to conclude that coercive cyber activity will never meet the level of a use of force because the instrumentality does not destroy the target in the traditional sense or that a cyberattack will always meet the use of force threshold."¹⁰⁶ Moreover, recent

at A1 (outlining Russia's use of cyberattacks on Georgia's Internet infrastructure); Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN, May 17, 2007, at 1 (outlining Russia's cyberattacks on Estonia in 2007).

¹⁰³ See DEPARTMENT OF DEFENSE OFFICE OF GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 18-20, 25 (May 1999), available at <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf> [hereinafter DOD OGC MEMO] ("It is far from clear the extent to which the world community will regard computer network attacks as 'armed attacks' or 'uses of force,' and how the doctrines of self-defense and countermeasures will be applied to computer network attacks.").

¹⁰⁴ U.N. Charter art. 39 ("the Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security").

¹⁰⁵ See Roscini, *supra* note 63, at 109-10 (stating that the Russian Federation supports a cyber disarmament agreement banning the development, production and use of dangerous information weapons. Further, the Russian Federation has declared that "'information weapons' can have 'devastating consequences comparable to weapons of mass destruction.' Therefore, 'the use of Information Warfare against the Russian Federation will categorically not be considered a non-military phase of a conflict whether there were casualties or not.'"). Compared to the military instrument, the cyber instrument is more accessible to both state and non-state actors. The cyber instrument presents the possibility of an asymmetric threat to inter-state relations because it could be used as a tool for states with fewer resources and less dependence on information technology and network infrastructure.

¹⁰⁶ See Jensen, *supra* note 98, at 222; see generally White House Cyber Policy *supra* note 3; and TALLINN MANUAL, *supra* note 3 (these examples of *opinio juris* and international scholarship advance the notion that uses of the cyber instrument can rise to the level of a use of force).

state practice and international scholarship have advanced the notion that cyber operations in this new battle space can rise to the level of a use of force.¹⁰⁷

Coercive use of the cyber instrument has been defined as “the sub-set of information warfare that involves actions taken place within the cyber world, [where t]he cyber world is any virtual reality contained within a collection of computers and networks.”¹⁰⁸ Coercive cyber activities by states fall into one of two categories.¹⁰⁹ First, a *cyberattack* would be a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.¹¹⁰ These operations are intended to penetrate another state’s computer and information systems or networks and have deleterious effects on those systems and the infrastructure they support, including altering, disrupting, or deceiving.¹¹¹ Second, *cyber exploitation* would be one state’s penetration of another’s systems and networks without a destructive payload. The exploitation may be in anticipation of a future cyberattack, but the operation does not cause any harm to the system or network. Cyberattacks are the most likely cyber operations to fall within the ambit of Article 2(4) and provide context for the application of Article 2(4) to the use of the cyber instrument.¹¹²

The lines of demarcation on the prevailing coercion continuum are also effective for categorizing coercive uses of the cyber instrument, such as cyberattacks. A cyberattack could be deemed to meet one of three categories: “first, as an action below the threshold of a use of force; second, an action that is equivalent to a use of force but short of an armed attack; or, third, as action that equates to an armed attack.”¹¹³ These lines of demarcation provide categories for characterizing coercive uses of the cyber instrument, but do not provide models or criteria to analyze and categorize any such uses.

¹⁰⁷ Koh, speech *supra* note 3, at 4 (“cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force”); TALLINN MANUAL *supra* note 3, R.11 (“a cyber activity constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force . . . acts that injure or kill persons or damage or destroy objects are unambiguously uses of force”).

¹⁰⁸ Raymond C. Parks & David P. Duggan, *Principles of Cyber Warfare*, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security (June 5-6, 2001), available at http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf.

¹⁰⁹ See Lin, *supra* note 71; NRC REPORT *supra* note 45.

¹¹⁰ TALLINN MANUAL, *supra* note 3, R. 30.

¹¹¹ Schmitt and Jensen refer to these operations as “Computer Network Attacks.” Schmitt, *supra* note 1, at 886; Jensen, *supra* note 98, at 208.

¹¹² See, e.g., Schmitt, *supra* note 1; Richardson, *supra* note 100; Richmond, *supra* note 100.

¹¹³ See Jensen *supra* note 98 at 207; Sharp *supra* note 98; see also *Nicar. v. U.S.*, *supra* note 78 ¶ 195 (distinguishing categories of uses of force including “mere frontier incident” which does not rise to the level of an armed attack); Murphy *supra* note 88.

Similar to use of force analysis in the physical domain, there are multiple models for use of force analysis in the cyber domain. The cyber domain models for use of force analysis are anchored in examining the extent of destructive physical effects or potential effects of cyberattacks. Although these models examine the effects of cyberattacks, they do not distinguish whether the effects are direct or indirect. Unlike the models for examining the use of the military instrument, the models for examining coercive uses of the cyber instrument have little to no state practice to measure their levels of efficacy or international acceptance because of the simultaneous challenges of recognizing the cyber operation, attributing it to the source, and pace of developing state practice and customary international law.¹¹⁴ The three proposed models for analyzing coercive uses of the cyber instrument are: 1) the analogous-to-instrument model; 2) effects-based model; and 3) a model similar to strict liability.¹¹⁵ Proponents of all three models agree that cyberattacks can rise to the level of an armed attack.¹¹⁶

First, using the “analogous-to-instrument model,” a cyberattack would be categorized as an armed attack if the effects of the damage in the physical domain could have been achieved only through the use of the armed instrument prior to the development of the cyber instrument.¹¹⁷ This model first examines the effects of the cyberattack in order to overlay the prevailing instrument-based model on the use of the cyber instrument. This “analogous-to-instrument” model would harmonize with the prevailing use of force analysis for traditional weapons.¹¹⁸ The U.S. and the legal experts who drafted the Tallinn Manual advocate for this model.¹¹⁹

Under the analogous-to-instrument model, it is possible for a cyberattack alone to rise to the level of an armed attack.¹²⁰ Koh and the Tallinn manual are

¹¹⁴ The White House Cyber Policy *supra* note 3; Koh speech *supra* note 3; and TALLINN MANUAL *supra* note 3 are the nascent formation of state practice reflecting customary international law.

¹¹⁵ See Paul Rosenzweig, *National Security Threats in Cyberspace*, A.B.A. STANDING COMM. & NAT. STRATEGY FORUM, Sept. 2009; Graham *supra* note 43; Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007) (Hollis’ “instrument-based” approach only looks to the means of the attack and not the consequences, whereas his “target-based” approach is similar to the strict liability model of Graham and Rosenzweig).

¹¹⁶ See Koh speech, *supra* note 3 (“we must articulate and build consensus around how it applies and reassess from there whether and what additional understandings are needed. Developing common understandings about how these rules apply in the context of cyberactivities in armed conflict will promote stability in this area”); Jensen, *supra* note 98, at 228-231.

¹¹⁷ See Rosenzweig, *supra* note 115; Graham *supra* note 43 (under this model, effects analogous to the use of chemical, biological, and other non-kinetic weapons that were previously deemed instruments of force are also armed attacks).

¹¹⁸ See Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT’L L.J. 179, 187 (2006) (citing BROWNLIE, *supra* note 86, at 362-63).

¹¹⁹ See White House Cyber Policy, *supra* note 3; Koh speech, *supra* note 3; TALLINN MANUAL, *supra* note 3.

¹²⁰ See Schmitt, *supra* note 1, at 904.

correct in emphasizing that it is not an unlawful use of force, but an armed attack which gives a state the right to respond in self-defense under Article 51.¹²¹ To reach the level of an armed attack, a cyberattack must have results that are kinetic parallels, including direct physical injury or damage to tangible property.¹²² This model analogizes the commonalities of the consequences of the use of armed force with the consequences of the use of the cyber instrument to determine whether or not the cyberattack reaches the level of a use of force or, more specifically, an armed attack.¹²³

Both the U.S. and the Tallinn analogous-to-instrument assessment of cyber operations look at several factors in establishing commonalities between the consequences of coercive acts rising to the level of use of force.¹²⁴ The U.S. would examine: “the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues.”¹²⁵

Likewise, the Tallinn Manual outlines eight non-exclusive factors. Although not formal legal criteria, these factors would be examined on a case-by-case basis using a holistic assessment of the circumstances of the incident to make the characterization.¹²⁶ First, and most importantly, severity examines the physical consequences of the cyber operation such as physical injury and destruction of property.¹²⁷ For a cyber operation to reach the level of a use of force, the severity of the physical harm must be consistent with that of an armed attack, such as death, destruction, or significant damage. Second, immediacy tracks the speed with which the coercive act ripens to full effect.¹²⁸ For a cyber use of force to rise to the level of an armed attack, the opportunity to achieve a peaceful resolution must be diminished because of the pace of the events. Third, directness examines the object of the use of force.¹²⁹ As with a traditional use of force, the focus of the cyberattack

¹²¹ Koh speech, *supra* note 3, at 4; TALLINN MANUAL, *supra* note 3, R. 13.

¹²² See Koh speech, *supra* note 3, at 4; TALLINN MANUAL, *supra* note 3, R. 13; Schmitt, *supra* note 1, at 904 (Schmitt points out that the “essence of an ‘armed’ operation is the causation, or risk thereof, of death or injury to persons or damage to or destruction of property and other tangible objects”).

¹²³ In the wake of the *Nicaragua* decision, the U.S. articulated the position that any illegal use of force can qualify as an armed attack triggering the right of self-defense. See TALLINN MANUAL, *supra* note 3, R. 11 cmt. 9 (citing Abraham D. Sofaer, *International Law and the Use of Force*, 82 AM. SOC’Y OF INT’L LAW PROCEEDINGS 420, 422 (1988)).

¹²⁴ Koh speech, *supra* note 3, at 4; TALLINN MANUAL, *supra* note 3, R. 13. Schmitt’s original analogous model used all but two of the Tallinn factors, military character of the operation and the extent of state involvement. Schmitt’s previous model was an expansion of Pictet’s use of force criteria: scope, duration, and intensity. See COMMENTARY OF THE GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN THE TIME OF WAR 583 (Jean S. Pictet ed., 1958).

¹²⁵ Koh speech, *supra* note 3, at 4. The U.S. has not further expressed the contours of these factors.

¹²⁶ Schmitt, *supra* note 100, at 20.

¹²⁷ TALLINN MANUAL, *supra* note 3, R. 11 cmt. 9.

¹²⁸ See TALLINN MANUAL, *supra* note 3, R. 11 cmt. 9; see also Schmitt, *supra* note 1, at 899-900.

¹²⁹ See *id.*

must be clear. Fourth, invasiveness examines the locus of the coercive act.¹³⁰ Despite potentially having similar effects, lawful economic acts generally take place outside of the target state's borders, but unlawful uses of armed force occur within the territory of the target state. The greater the intrusion on the rights of the target state equates to a greater disruption to international stability. Fifth, measurability examines the difficulty in determining the consequences of the attack.¹³¹ With the use of military instrument, measuring the consequences is much simpler than determining the effects of other coercive acts, such as economic sanctions. A use of the cyber instrument is more likely to be characterized as rising to the level of a use of force if the effects are more identifiable and quantifiable.¹³² Sixth, a connection between the cyber operation and military operations increases the likelihood of characterizing the cyber activity as a use of force.¹³³ Seventh, similar to the military character of the operation, the greater the extent of state involvement in the cyber operation the increased likelihood that the operation will be characterized as a use of force.¹³⁴ Finally, eighth, as the consequences of violent uses of the military instrument are presumptively illegitimate, the consequences of a use of the cyber instrument must be presumptively illegitimate to rise to the level of an armed attack.¹³⁵

Although using an "analogous-to-instrument" approach is consistent with the current instrument-based analysis, it would be a change to established interpretation, and more gray areas of interpretation would persist until state practice and *opinio juris* form.¹³⁶ By examining the physical effects of a cyberattack, the analogous-to-instrument model is an evolution of the instrument-based understanding of force that is prohibited by Article 2(4). Although consistent with the customary interpretation in applying an earlier generation's analysis to a new generation of weapons, a multi-factor model may be inefficient for states and the international community to analyze a coercive use of the cyber instrument. The time necessary to complete a full analysis may be purposeful in maintaining international stability and determining the proper course of action. However, the analogous-to-instrument model fails to address both the full-spectrum of the cyber threat and non-tangible consequences from the use of the cyber instrument, such as loss of confidence in an economy.¹³⁷

¹³⁰ See *id.*

¹³¹ *Id.*

¹³² *Id.*

¹³³ TALLINN MANUAL, *supra* note 3, R. 11 cmt. 9.

¹³⁴ *Id.*

¹³⁵ See TALLINN MANUAL, *supra* note 3, R. 11 cmt. 9; see also Schmitt, *supra* note 1, at 899-900.

¹³⁶ See, e.g., Schmitt, *supra* note 100, at 20; Schmitt, *supra* note 1, at 902.

¹³⁷ See Graham, *supra* note 43, at 91 (citing THOMAS WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 41-44 (2000)).

The second analytical model is an effects-based model, or consequence-based model. The effects-based analysis focuses on the overall effect of the cyberattack on the target state instead of the effect's parallel to armed attacks.¹³⁸ The effects-based model addresses the broader spectrum of cyberattacks and their aggregate direct and indirect effects. This is an expansion beyond the prevailing definition of force in kinetic terms because it would include more than physical effects.¹³⁹ Contrary to the customary model, where blockades and sanctions with similar effects are treated as disparate acts of coercion because of the instrument used, the effects-based model only examines the consequences of a cyberattack. The effects-based model looks at the scale and effects of the cyberattack on the target state.¹⁴⁰ Although the effects-based model addresses the broader threat posed by the use of the cyber instrument, its inconsistencies with the customary interpretation of Article 2(4), the *travaux préparatoires*, and state practice are problematic.

The experts at Tallinn addressed instances where the effects of coercive use of the cyber instrument do not have a clear kinetic parallel. As highlighted above, the U.S. has asserted the position that any use of force rises to the level of an armed attack, triggering the right of self-defense.¹⁴¹ As outlined in the Tallinn Manual, however, a coercive use of the cyber instrument that lacks a clear kinetic parallel could rise to the level of a use of force without triggering the right to self-defense.¹⁴²

Dr. Walter Gary Sharp has advocated for a third analytical model similar to a strict liability approach.¹⁴³ Under this model, any cyberattack conducted by a state actor “that intentionally causes *any* destructive effect within the sovereign territory of another state is an unlawful use of force that may constitute an armed attack.”¹⁴⁴ Any cyberattack on a state’s critical infrastructure would be deemed an armed attack per se, regardless whether or not the attack is successful.¹⁴⁵ Cyberattacks on non-critical infrastructure would be presumed to have hostile

¹³⁸ See Rosenzweig, *supra* note 115; Graham, *supra* note 43.

¹³⁹ *Id.* (Graham cites a May 1999 Department of Defense Office of General Counsel memorandum as evidence that the U.S. has adopted this approach, which contrasts the U.S. approach to kinetic uses of force. *But see* DoD OGC MEMO, *supra* note 103, at 18-20, 25 (analyzing potential scenarios similar to the analogous-to-instrument approach)).

¹⁴⁰ This language tracks with the *Nicaragua* decision. Schmitt, *supra* note 100, at 19.

¹⁴¹ See Koh speech, *supra* note 3.

¹⁴² See TALLINN MANUAL, *supra* note 3, R. 11 cmt 4 (this position is consistent with the *Nicaragua* decision).

¹⁴³ See SHARP, *supra* note 98.

¹⁴⁴ See *id.* at 95.

¹⁴⁵ See Rosenzweig, *supra* note 115, at 14.

intent; thus, based on the scope, duration and intensity of the attack, the victim state may consider such actions an armed attack.¹⁴⁶

The strict liability model for the use of the cyber instrument is less consistent with state practice for determining prohibited force under Article 2(4) than the analogous-to-instrument model. Sharp's model would be an alteration of the scope of Article 2(4) because it would examine both the instrument and the target. Although Sharp's model seemingly establishes clear lines, its analysis would turn on other problematic determinations such as whether infrastructure is "critical to a state's vital national interests."¹⁴⁷ This definition of critical infrastructure could capture economic and political coercion that is not traditionally prohibited as force under Article 2(4). As discussed above, economic and political coercion have gained acceptance through state practice as permissible forms of coercion.

The analogous-to-instrument and strict liability models would serve different purposes in international law. Evolving the interpretation of Article 2(4) towards the "analogous-to-instrument" model would be an easier evolution of Article 2(4) interpretation because it is the most consistent of the three models with the customary interpretation. Unless the customary interpretation evolves, it may lose favor in the near future as coercive use of the cyber instrument increases.¹⁴⁸ Nevertheless, critics argue that the analogous-to-instrument model's narrow construction may restrain a nation-state's ability to respond aggressively, and will have the unintended consequence of encouraging more coercive uses of the cyber instrument in order to determine where the line of demarcation for triggering a forceful response falls on the coercion continuum.¹⁴⁹ An effects-based analytical framework looks at the scope and magnitude of the effects on the victim state. Such an evolution would not be consistent with the customary interpretation of Article 2(4). Evolving the interpretation of Article 2(4) towards Sharp's "strict liability" model would serve as a deterrent to other bad actors by lowering the threshold for what level of cyberattack would elicit a forceful response.¹⁵⁰ However, Sharp's model is the least consistent with the prevailing interpretation--thus a more difficult evolution.

All three of the above models for analyzing the coercive use of the cyber instrument would evolve the prevailing definition of force prohibited by Article 2(4). But international law and state practice are not static.¹⁵¹ A nation must have the right to respond to external threats, regardless of instrument. Article 2(4) and

¹⁴⁶ See SHARP, *supra* note 98, at 132.

¹⁴⁷ See SHARP, *supra* note 98, at 131.

¹⁴⁸ See Jensen, *supra* note 98, at 228.

¹⁴⁹ See *id.* at 228.

¹⁵⁰ See *id.* at 228.

¹⁵¹ See, e.g., Koh speech, *supra* note 3; TALLINN MANUAL, *supra* note 3; Schmitt, *supra* note 100.

the U.N. Charter have maintained their value to the international system because of the flexibility they provide to states in evolving accepted definitions and state practice without breaking the spirit of the text or the integrity of the international system. As the use of the cyber instrument continues to develop as a means of inter-state coercion, state practice and international understanding of force will also evolve.

Stuxnet provides an opportunity for the international community to evolve the customary interpretation of Article 2(4)'s prohibition against the use of force to include the coercive use of the cyber instrument. One step in the evolution of the interpretation of Article 2(4)'s prohibition against force may be the international response to Stuxnet. Although not a violation under the current instrument-based definition, Stuxnet would be a use of force prohibited by Article 2(4) under each of the above discussed models.

V. Stuxnet and Article 2(4) of the U.N. Charter

Stuxnet presents a challenge to the customary interpretation of what force is prohibited under Article 2(4). This challenge may be an opportunity to maintain the relevancy of Article 2(4) by evolving the customary interpretation of force to include coercive uses of the cyber instrument. The purposes of the prohibition against force include maintaining international peace and preventing destructive intervention by one state into the affairs of another.

By targeting and destroying critical infrastructure in the Iranian nuclear complex, Stuxnet was a coercive use of the cyber instrument that had effects in the physical world. Under current state practice and definitions of what force is prohibited under Article 2(4), however, Stuxnet was not a use of force. To remain faithful to the purposes of the U.N. Charter, state practice and international understanding must adapt to the realities of the destructive use of the cyber instrument by evolving the definition of force prohibited by Article 2(4). Again, the analysis below assumes Stuxnet has been attributed to the responsible state.

Coercive uses of the cyber instrument evade the customary interpretation of Article 2(4). Despite the physical destruction to the Iranian nuclear complex, Stuxnet would not be considered a use of force and would not enable Iran to respond legitimately in self-defense.¹⁵²

The previously discussed models offer a way to analyze uses of cyber instrument that evolves the customary interpretation Article 2(4) to relevancy in the cyber age while remaining consistent with the purposes of the U.N. Charter. Under

¹⁵² Legitimate within the parameters of Art. 51 of the U.N. Charter.

all three models, Stuxnet would be a use of force because of the physical destruction caused to Iran's critical infrastructure.¹⁵³ The Tallinn experts, however, could not agree that Stuxnet was equivalent to an armed attack triggering the right to respond with force in self-defense.¹⁵⁴

Using the "analogous-to-instrument" model, Stuxnet is a use of force because the malware caused the destruction of centrifuges at Natanz that could have been achieved previously only through the use of the military instrument. The policy outlined by Koh, however, offers the U.S. the flexibility to characterize coercive uses of the cyber instrument to be consistent with both its stated policy and the diplomatic needs. Given the diplomatic and national security implications, however, the U.S. has not stated its position characterizing whether Stuxnet is a use of force.

Characterizing Stuxnet as a use of force is less complicated for the legal experts who drafted the Tallinn Manual who do not have the considerations of formalizing state policy having lasting ramifications. For the Tallinn experts, Stuxnet is a use of force, but they were unable to unanimously agree that it equated to an armed attack.¹⁵⁵ Stuxnet satisfies the other criteria for showing the commonalities between a cyber use of force and an armed use of force, but, for some of the Tallinn experts, Stuxnet did not meet the immediacy requirement to characterize the cyber operation as an attack triggering the right to self-defense.¹⁵⁶ For some of the Tallinn experts, there is difference in what meets the immediacy requirement between characterization as a use of force versus an armed attack.¹⁵⁷ The sooner the effects of the cyber operation manifest in the victim state, the more likely the operation will be characterized as a use of force.¹⁵⁸ According to some of the Tallinn experts, the target state must identify operation, injury, or damage contemporaneously to satisfy the armed attack requirement.¹⁵⁹ Immediacy is satisfied for characterization as a use of force because Stuxnet had infiltrated and destroyed Natanz centrifuges before Iran was even aware of the malware, or at least able to mitigate it. But if the cyber operation, injury, damage, or initiating state has not been identified by the target state, the immediacy requirement for characterization as armed attack is not met.¹⁶⁰ Stuxnet satisfies the directness criteria because the malware was designed specifically for the fuel enrichment plant at Natanz, and it successfully deployed its destructive payload on that target. The malware infiltrated Iranian systems and networks en route to its intended target,

¹⁵³ See TALLINN MANUAL, *supra* note 3, R. 10.

¹⁵⁴ See TALLINN MANUAL, *supra* note 3, R. 22.

¹⁵⁵ See TALLINN MANUAL, *supra* note 3, R. 13 cmt. 13.

¹⁵⁶ See TALLINN MANUAL, *supra* note 3, R. 15 cmt. 10.

¹⁵⁷ See TALLINN MANUAL, *supra* note 3, R. 15 cmt. 9.

¹⁵⁸ See TALLINN MANUAL, *supra* note 3, R. 13 cmt. 11(d).

¹⁵⁹ See TALLINN MANUAL, *supra* note 3 R. 15 cmt. 10.

¹⁶⁰ *Id.*

satisfying the invasiveness criterion. The effect of Stuxnet is measurable by the number of centrifuges destroyed. Finally, the infiltration and exploitation of Iranian computer systems controlling critical nuclear infrastructure would be presumptively unlawful both amongst the international community and domestically within Iran.

As discussed above, the analogous-to-instrument analytical model is reflective of the current state of international law, but it may not be consistent with future state practice. Although the “analogous-to-instrument” model examines the commonalities of the effects of cyberattacks with the effects of armed attacks, states may desire to place uses of the cyber instrument on the coercion continuum based on the overall effects of the attack or the target of the attack. , The “effects-based” model and the “strict liability model” would both characterize Stuxnet as a use of force equivalent to an armed attack.

Applying the effects-based model, Stuxnet would be a violation of Article 2(4)'s prohibition of the use of force because of the overall physical and economic effects of the malware on the Iranian nuclear complex. The effects-based model looks at the scope and magnitude of the cyberattack on the target state. With Stuxnet, the scope and magnitude of the effects include the infiltration and exploitation of computer systems and the destruction of more than ten percent of the centrifuges at Iran's largest nuclear fuel enrichment plant. Based on the scope and magnitude of the effects of Stuxnet on Natanz, the attack would be a use of force prohibited by Article 2(4) equivalent to an armed attack.

Sharp's model provides the clearest approach for categorizing Stuxnet as a use of force equivalent to an armed attack. Sharp's model would deem Stuxnet an armed attack because the malware targeted Iranian critical infrastructure. Deeming any use of the cyber instrument targeting critical infrastructure to be per se an armed attack is a departure from the current definition of force under Article 2(4). Despite this departure, Sharp's model offers a clear approach to categorizing interstate coercive uses of the cyber instrument under Article 2(4).

All three models would evolve the customary definition of force prohibited by Article 2(4), but further state practice will determine whether an evolution in the interpretation of the force prohibited by Article 2(4) will occur and how coercive uses of the cyber instrument will be viewed.¹⁶¹ From the perspective of states whose critical infrastructure is dependent on information technology systems, the customary interpretation is problematic because cyberattacks against critical infrastructure evade prohibition by Article 2(4). Conversely, for these technology-dependent states, the strict liability model is attractive because it

¹⁶¹ See DoD OGC MEMO, *supra* note 103 (“international law in this area [the use of the cyber instrument] will develop through the actions of nations and through the positions the nations adopt publicly as events unfold”).

provides deterrence. Given the speed of cyberattacks, the multi-factor model is less attractive because it may be inefficient in analyzing and responding to cyberattacks. Contrastingly, states with offensive cyber capabilities may want the ability to use the cyber instrument as a coercive tool for inter-state relations because of the problem of attribution; thus, the diminished possibility of accountability or retribution. For states with offensive cyber capabilities, the customary interpretation is sufficient because it allows the coercive use of the cyber instrument while any evolution could restrict the use of a means of inter-state coercion. State practice, particularly by internationally powerful states, will determine whether an evolution of the customary interpretation of Article 2(4) occurs.¹⁶²

The purpose of such an evolution would be to establish a norm for state behavior, and state practice will determine whether such an evolution becomes accepted as an international norm.¹⁶³ According to reports, powerful states, such as the United States, Russia, and China, are both dependent on information technology and have used the cyber instrument as a coercive tool.¹⁶⁴

In the event that attribution of coercive uses of the cyber instrument becomes less difficult, internationally powerful states may be inclined to accept an evolution of the customary interpretation of force prohibited by Article 2(4) and establish a norm restricting the coercive use of the cyber instrument in order to protect their networks and critical infrastructure.¹⁶⁵ But, these powerful states would likely still want the option to use the cyber instrument as a means of inter-state coercion. Similar to how humanitarian intervention has been viewed by some as an “excusable breach” of Article 2(4) with regard to the use of the armed instrument,¹⁶⁶ states may determine that circumstances may warrant excusable breaches of the norm against the coercive use of the cyber instrument. To the state responsible for Stuxnet, the Iranian nuclear program may have presented sufficient circumstances for such an “excusable breach.”

¹⁶² See DoD OGC MEMO, *supra* note 103. The DoD OGC MEMO could be read as state practice because it indicates how the U.S. Department of Defense would analyze coercive uses of the cyber instrument.

¹⁶³ See White House Cyber Policy, *supra* note 3 (outlining the need to establish norms for the international community).

¹⁶⁴ See Elliott, Markoff and Traynor cited *supra* note 102, Jensen *supra* note 98, at 207-208; Todd Beamon, *Rep Rogers: China and Russia Conduct 'Vicious' Cyberattacks on U.S.*, NEWSMAX (May 28, 2013), <http://www.newsmax.com/newsfront/rogers-china-russia-cyberattacks/2013/05/28/id/506756>. The difficulty of attribution makes advocating for an evolution seem wasteful for a number of reasons. First, states could agree to a revised interpretation and still use the cyber instrument with impunity without fear of identified. Second, states who still wish to use the cyber instrument coercively may be reluctant to agree to a norm they intend to violate.

¹⁶⁵ See generally White House Cyber Policy, *supra* note 3; Koh Speech, *supra* note 3.

¹⁶⁶ See Jane Stromseth, *Rethinking Humanitarian Intervention: The Case for Incremental Change*, in HUMANITARIAN INTERVENTION: ETHICAL, LEGAL, AND POLITICAL DILEMMAS (J. L. Holzgrefe & Robert Owen Keohane eds., 2003).

Stuxnet presents an opportunity to evolve the customary interpretation of Article 2(4)'s prohibition against the use of force with respect to inter-state coercive uses of the cyber instrument because of the scope of the operation, nature of the target, and publicity of its effects, enabling study and discussion without attributing its source. The customary interpretation of Article 2(4) is ill-suited for the effects of coercive uses of the cyber instrument, but analytical models that address the lacunae are available.¹⁶⁷ These models vary in methodology and consistency with current Article 2(4) understanding. Despite the differences in methodology, each of the models would deem Stuxnet and its effects on the Iranian nuclear complex as a use of force equivalent to an armed attack.¹⁶⁸ State practice will determine whether the customary interpretation of Article 2(4) will evolve to include coercive uses of the cyber instrument.¹⁶⁹

VI. Conclusion

The Stuxnet malware attack is an evolutionary opportunity for applying Article 2(4) and international law of *jus ad bellum* to the use of the cyber instrument. The malware's complexity, sophistication, and destruction serve as a warning of the magnitude of this method of inter-state coercion unforeseen at the time of the drafting of the U.N. Charter.

The textual ambiguity and flexibility of Article 2(4) has enabled it to remain relevant in the regulation of international relations, even if its definition is unsettled. Article 2(4)'s prevailing definition turns on the instrument of coercion. If it is armed, then it is force. However, as the *Nicaragua* case demonstrates, a use of force and an armed attack are at different points on the coercion continuum, but exactly where on that continuum is unclear.

To remain relevant in response to coercive uses of the cyber instrument, the customary interpretation of force prohibited by Article 2(4) should evolve. Stuxnet provided the international community an opportunity to begin to evolve the customary interpretation of Article 2(4)'s prohibition against the use of force to include coercive uses of the cyber instrument. Three proposed analytical models present different approaches to evolving the definition of Article 2(4) to address the challenges posed by the use of the cyber instrument: the analogous-to-instrument,

¹⁶⁷ See Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force,"* 67 JOINT FORCES Q. 40, 40-48 (2012) (highlighting that there are still gaps to be worked out with the analogous-to-instrument analysis, specifically, that Stuxnet would not have been characterized a use of force if the malware had simply made the centrifuges work slower or less efficiently instead of destroying them).

¹⁶⁸ See Michael Schmitt, *Classification of Cyber Conflict*, 17 J. OF CONFLICT & SEC. L., 245, 252 (2012). But see TALLINN MANUAL, *supra* note 3, R. 13 cmt. 13 (indicating that the international group of experts were unable to definitively conclude that the Stuxnet attack rose to the level of an armed attack because of legal and practical difficulties in labeling a cyber operation).

¹⁶⁹ See, generally TALLINN MANUAL, *supra* note 3; Koh speech, *supra* note 3, at 2.

effects-based, and strict-liability models. The analogous-to-instrument model has gained the most favor, but has not been firmly established as customary international law.¹⁷⁰ While these models vary in their methodology and their consistency to the current state of international law, each of the three proposed models would deem Stuxnet as a use of force, and two would characterize it equivalent to an armed attack. Stuxnet could be an opportunity to evolve the prevailing interpretation of Article 2(4)'s prohibition against the use of force to include coercive uses of the cyber instrument, but such an evolution is unlikely to happen until attribution becomes less difficult. The model proposed by the Tallinn experts is the soundest of the three because of its consistency with the customary interpretation and application of Article 2(4) and its support amongst the international legal community. Technologically-dependent states would support an evolution of the interpretation in order to protect their critical infrastructure. Unless the problem of attributing coercive uses of the cyber instrument is solved, however, powerful states, even if technologically-dependent, are unlikely to support evolving the interpretation of Article 2(4) because they are likely to continue to use the cyber instrument as a means of inter-state coercion.

¹⁷⁰ See, generally TALLINN MANUAL, *supra* note 3; Koh speech, *supra* note 3.

DEPARTMENT OF DEFENSE WATER RIGHTS: A PROPOSED POLICY

Captain Michael T. Palmer, JAGC, USN*

I. Introduction

Water is a scarce resource throughout the western states and in ever-increasing parts of the eastern United States.¹ Increasing water use demands on existing and finite water supplies, pollution, and concerns about global climate change have focused increased attention to water resource appropriation, management, and conservation. One entity increasingly concerned about water uses and resources is the Federal Government, including the Department of Defense (DoD). With installations ranging from industrial shipyards, to large fleet naval stations, to airfields, ranges, and research, development, and testing facilities, the DoD currently relies on groundwater withdrawals and surface water diversions to either supplement or meet their growing water needs. These self-supplied water acquisitions and uses are often exercised concurrent with, and occasionally contrary to, traditionally recognized state and local authorities to oversee, manage, and equitably distribute surface and groundwater natural resources located within their jurisdictions. Where water resources have been, or remain, relatively plentiful, federal/state conflicts concerning access and use have either been non-existent or the parties have negotiated workable solutions. In areas of traditional water scarcity, usually in the western United States,

* The author is an active duty captain in the Navy Judge Advocate General's Corps and an adjunct assistant professor at Old Dominion University. Captain Palmer has served as environmental counsel to both the Chief of Naval Operations (Installations and Environment), Commander, U.S. Fleet Forces Command (Sonar Integrated Coordinating Group), and Regional Commander, Navy Region Mid-Atlantic, Norfolk, VA. He has a BA degree from the University of Massachusetts; a Juris Doctorate from Suffolk University; and a Masters of Law degree in Environmental Law from The George Washington University. In addition to lecturing on the U.S. Navy's Sonar Protection Challenge as part of the Naval Postgraduate School's Mennecken Lecture Series, Captain Palmer he has written several articles including *Regulating Ocean Noise: A Non-traditional Threat to Maritime Security* (2009); *The Chesapeake Bay Restoration Act of 2000: New Requirements for Federal Agencies* (2004), *The Regional Haze Rule: EPA's Next Phase in Protecting Visibility under the Clean Air Act* (2001); and *Unwrapping the ROE Axle* (2004). The opinions expressed herein are those of the author and are not necessarily representative of those of the U.S. Department of Defense or the United States Navy.

¹ Policy Memorandum, Office of the Asst. Sec'y of the Army (Installations, Logistics, and Environment), subject: Policy Guidance on Water Rights at Army Installations in the United States (24 Nov. 1995) [hereinafter Asst. Sec'y of the Army Memorandum Water Rights] (Copy on file with author).

conflict potential is understandably heightened. This often forces DoD installations into full or partial compliance with state or local requirements or leads to undesirable disagreement between state and local officials. Going to the very core of federalism, these tensions and potential for political and judicial conflict will continue to exacerbate as state and local governments respond to decreasing water availability by tightening their regulatory controls over water allocation, including federal agency acquisition and uses.

Despite this conflict, there is currently no comprehensive federal “water use” statute, Presidential Executive Order, or DoD regulatory directive guidance addressing how DoD installations can ensure continued access to water to meet their statutory missions, immune from state or local control. Absent such a policy, DoD installations are left on their own to either navigate a labyrinth of often inconsistent state and local water allocation management water programs (water program) or assert federal sovereignty and claim immunity from state or local water allocation management requirements. Opting to comply with state and local regulation, despite no valid waiver of sovereign immunity, presents many challenges. These challenges include processing or extraction fees, conservation-based use limitations or prohibitions, and administrative or judicial stream adjudication procedures. DoD installations must make significant policy considerations when determining the breadth of permissible rights that they wish to assert, the applicability and extent of state or local allocation programs to federal agencies, the quantification of current and future water rights, and the choice of procedures and forums in which to adjudicate federal water rights.

Recognizing the need for a uniform water rights policy, the DoD has recently directed a survey of individual installation and activity historic and anticipated future water uses.² This is the first step of a DoD water use and water resource vulnerability assessment to evaluate its current and future capabilities to meet its statutory defense missions in light of potential and foreseeable resource reductions and state or local restrictions or prohibitions. The assessment will predictably reveal an unacceptable vulnerability to future statutory mission execution. This, in turn, will require a comprehensive DoD water use policy to ensure adequate protection of historic and future federal self-supplied water use needs.

² Memorandum from Office of the Under Sec’y of Def., to Asst. Sec’y of the Army (Installations, Logistics, and Environment) et al., subject: Water Rights and Water Resources Management on Dep’t of Def. Installations and Ranges in the United States and Territories (23 May 2014) [hereinafter Water Rights Memo].

This article proposes such a policy. It examines the rights and limits of DoD installations to appropriate and use self-supplied water withdrawals (acquisition by groundwater withdrawals or surface water diversions) on federal lands within the United States and its territories. It will not address installation water acquired through rental or lease agreements or other means of public-supply delivery. Part I acquaints the reader with introductory general information on the historical and legal regimes governing water allocation in the United States. Specifically, it focuses on the unique status of federal agencies as water appropriators and users and the conflict with traditionally recognized state rights over the allocation and use of water as a natural resource. Part II summarizes the author's proposed DoD regulatory policy, which is premised on the Coastal Zone Management Act's Federal Consistency requirements. This policy addresses acquisition of current and future DoD water needs for mission accomplishment, affords appropriate deference to state and local water allocation and use interests, and, equally important, preserves federal sovereign immunity from state and local regulation, enforcement, and detrimental water use prohibitions or restrictions.

II. Water Rights for the Federal Government: A Conflict Among Sovereigns

To provide requisite context for Part II's proposed DoD policy discussion, this section provides a summary of the basics underpinning the conflict between federal agencies and state governments over water allocation and use. It briefly notes the lack of federal water rights statutory law, discusses Congress's historical deference to state and local regulation of water as a natural resource, and reviews the development of state water allocation regimes and federal common law water rights. It then analyzes the sovereign immunity of federal agencies from state and local water allocation requirements and enforcement and concludes that interim DoD agency regulatory guidance is needed to ensure DoD access to sufficient allocations to meet its current and future water needs.

A. Federal “Ownership” of Unappropriated Water

Federal law does not recognize an ownership interest in unappropriated water. Unappropriated water, similar to wild animals, has been viewed as *res nullius* – the property of no one – until it has been captured.³ In *Hughes v. Oklahoma*, the Supreme Court noted that concepts of ownership of or title to natural resources such as natural gas, minerals, landfill areas, birds, fish and other wildlife is a “legal fiction” that merely expresses legitimate state regulatory interests in the conservation and protection of its natural resources.⁴ As one commentator has noted:

The state and the federal government share an interest in the proper regulation of water. Neither ‘owns’ unappropriated water, but each has the power to use it and to regulate its use The important question is whether federal rules of capture apply to the United States. In other words, the issue is whether Congress has established a federal regulatory jurisdiction over federal appropriations [of water] or has recognized the inherent regulatory jurisdiction of the state and adapted federal policies to it.⁵

Thus, a state’s power over its waters, as over other natural resources, is based on the state’s police powers and is subject to ordinary constitutional limitations such as the Commerce, Property, and Defense Clauses. This interpretation of the nature of the states’ and federal government’s interests in unappropriated water is consistent with the approach the Supreme Court has taken in cases involving the use or disposition of water in the Western states.⁶ Thus, the question is not one of competing ownership in the traditional sense of

³ See Frank J. Trelease, *Government Ownership and Trusteeship of Water*, 45 CAL. L. REV. 638, 643 (1957).

⁴ 441 U.S. 322, 334 (1979) (quoting *Toomer v. Witsell*, 334 U.S. 385, 402 (1948) (“The whole ownership theory, in fact, is now generally regarded as but a fiction expressive in legal shorthand of the importance to its people that a State have the power to preserve and regulate the exploitation of an important resource.”)). *Hughes* overruled *Geer v. Connecticut*, 161 U.S. 519 (1896) (state owns all natural resources).

⁵ Memorandum from Theodore B. Olson, Assistant Attorney General, Office of Legal CounselI, U.S. Department of Justice, to Carol E. Dinkins, Assistant Attorney General, Land and Natural Resources Division, subject: Federal “Non-Reserved” Water Rights, 56 (16 June 1992) [hereinafter “DoJ Memo”] (Copy on file with author) (quoting Comment, *Federal Nonreserved Water Rights*, 48 U. CHI. L. REV. 758, 772 (1981) (footnotes omitted)).

⁶ See, e.g., *United States v. Rio Grande Dam & Irrigation Co.*, 174 U.S. 690 (1899).

“fee interest,” but of competing regulatory jurisdiction – either under the state’s police powers or under the federal government’s constitutional powers.⁷

B. Congress's Historical Deference to State Sovereignty for Water Rights

There is no federal “water use” statute, Presidential Executive Order, or DoD regulatory directive guidance providing authority for DoD installations to acquire and use water as a function of installation land ownership or other property rights. Historically, Congress has deferred to state and local authorities when it comes to allocation and use of water as a natural resource.

Congress, with judicial concurrence through statutory interpretation, has deferred to the States’ authority to regulate water acquisition and usage.⁸ In a series of federal statutes designed to encourage settlement and private development in western territories and states, Congress repeatedly and explicitly deferred to the respective States to determine how to regulate water appropriation and use.⁹ In the Mining Act of 1866, Congress confirmed water rights for mining, agriculture, and other uses that had been acquired by private parties on public land shall be regulated under local customs, laws, and court decrees.¹⁰

In the Desert Land Act of 1877, Congress reconfirmed its deference to local customs and procedures for appropriation of water on public lands

⁷ See, e.g., *Sporhase v. Nebraska*, 458 U.S. 941, 951 (1982) (articulating that state ownership of groundwater is a ‘legal fiction’ and groundwater is an article of commerce subject to the Commerce Clause barring Nebraska’s attempt to regulate it.); *Kleppe v. New Mexico*, 426 U.S. 529, 537 (1976) (stating that ownership of wild horses and burros on federal land is irrelevant to the scope of the Federal Government’s authority under the Property and General Welfare Clauses to protect those horses and burros).

⁸ Michael G. Proctor, *Section 10 of the Rivers and Harbors Act and Western Water Allocations—Are the Western States Up a Creek Without a Permit?* 10 B.C. ENVTL. AFF. L. REV. 111, 119 (1982). See *United States v. New Mexico*, 438 U.S. 696, 699 (1978) (noting that Congress has seldom expressly reserved water for use on withdrawn lands); *United States v. Fallbrook Pub. Util. Dist.*, D.C., 165 F. Supp. 806, 831 (S.D. Cal. 1958) (“There is no body of federal water law.”).

⁹ *United States v. New Mexico*, 438 U.S. at 701 n.5 (“See *Hearings on S. 1275 Before the Subcomm. on Irrigation & Reclamation of the S. Comm. on Interior & Insular Affairs*, 88th Cong., 2d Sess., 302–10 (1964) (App. B, supplementary material submitted by Sen. Kuchel), listing 37 statutes in which Congress has expressly recognized the importance of deferring to state water law, from the Mining Act of 1866, § 9, 14 Stat. 253, to the Act of Aug. 28, 1958, § 202, 72 Stat. 1059, stating Congress’s policy to ‘recognize and protect the rights and interests of the State of Texas in determining the development of the watersheds of the rivers . . . and its interests and rights in water utilization and control.’”).

¹⁰ D. Craig Bell & Norman K. Johnson, *State Water Laws and Federal Water Uses: The History of Conflict, the Prospects for Accommodation*, 21 ENVTL. L. 1, 23–24 (1991).

declaring “the right to the use of [western states’] waters by claimant[s under the Act] shall depend upon bona fide prior appropriation.”¹¹ The Desert Land Act further stated:

[A]ll surplus water over and above such actual appropriation and use, together with the water of all lakes, rivers and other sources of water supply upon the public lands and not navigable, shall remain and be held free for the appropriation and use of the public for irrigation, mining, and manufacturing purposes subject to existing rights.¹²

In *California Oregon Power Co. v. Beaver Portland Cement Co.*, the Supreme Court held that the effect of the Desert Land Act was to “sever” the land and water estates in the public domain providing for state, not federal, control of water rights.¹³ Congress directed that water rights be established under state and territorial laws.¹⁴

In its Reclamation Act of 1902,¹⁵ a federal law that funded various irrigation projects in the United States, Congress expressly declared its deference to state water law and the obligation of the United States to abide by state law with reference to water rights, by including a savings clause that states:

Nothing in this Act shall be construed as affecting or intending to affect or in any way interfere with the laws of any state or territory relating to the control, appropriation, use, or distribution of water used in irrigation, or any vested right acquired there under, and the Secretary of the Interior, in carrying out the provisions of this Act, shall proceed in conformity with such laws¹⁶

¹¹ *Id.* (quoting Act of March 3, 1877, ch. 107 (current version at 43 U.S.C. § 321 (1988)); *Cal. Or. Power Co. v. Beaver Portland Cement Co.*, 295 U.S. 142, 156 (1935).

¹² 43 U.S.C. § 321 (2015).

¹³ *Bell & Johnson*, *supra* note 10, at 25 (citing *Cal. Or. Power Co.*, 295 U.S. at 153–58; *United States v. New Mexico*, 438 U.S. at 702).

¹⁴ *Bell & Johnson*, *supra* note 10, at 24 (citing *Cal. Or. Power Co.*, 295 U.S. at 162); *See also* *Ickes v. Fox*, 300 U.S. 82, 94–96 (1937); *Nevada v. United States*, 463 U.S. 110, 123–24 (1983).

¹⁵ 43 U.S.C. § 372 (2015).

¹⁶ *Bell & Johnson*, *supra* note 10, at 25 (quoting 43 U.S.C. § 372 (1988)). For similar “savings” clauses, *see* 33 U.S.C. § 1251(g) (1987) (Clean Water Act); 16 U.S.C. § 821 (1988) (Federal Power Act). The Supreme Court has previously detailed Congress’s repeated deference to state water law. *United States v. New Mexico*, 438 U.S. 696, 701 n.5 (1978) (citing legislative history discussing such deference); *see also* *California v. United States*, 438 U.S. 645, 653–79 (1978) (discussing this congressional deference). The Supreme Court has generally upheld this Congressional deference to state water law. *See, e.g.*, *Cal. Or. Power Co.*, 295 U.S. 142 (1935); *Kansas v. Colorado*, 206 U.S.

C. State Water Allocation Regimes: Riparian and Appropriative

In light of Congress's deference to state regulation of water, and absent federal guidance on federal water use, DoD installations look to state regulatory regimes to acquire and maintain water for mission purposes. A summary of these regimes is provided below.

Because of different climatic, topographic and geographic conditions and the differing demands of agricultural and economic development, the arid and semi-arid western states have developed different legal doctrines and administrative machinery governing water rights. Water rights are largely a creature of private property rights augmented by state and federal water law governing the allocation and use of surface and groundwater. Historically, water rights were acquired in one of two ways: as incidents of ownership of riparian property and by appropriation.¹⁷ The riparian rights doctrine generally prevails in the eastern United States, while the appropriation doctrine is commonplace in the arid and semi-arid western states.¹⁸

46 (1907); *cf.* *United States v. Rio Grande Dam & Irrigation Co.*, 174 U.S. 690, 703 (1899) ("Although this power of changing the common law rule as to streams within its dominion undoubtedly belongs in each state, yet two limitations must be recognized: first, that, in the absence of specific authority from Congress, a state cannot, by its legislation, destroy the right of the United States, as the owner of lands bordering on a stream, to the continued flow of its waters, so far at least, as may be necessary for the beneficial uses of the government property; second, that it is limited by the superior power of the general government to secure the uninterrupted navigability of all navigable streams within the limits of the United States.").

¹⁷ Under the "American Rule," riparian owners acquire a right of reasonable use, not only to in-stream flow, but also for consumptive purposes. Where a state recognizes riparian water rights, the United States, as a riparian landowner, may assert those rights. *See* Rymn J. Parsons, *Groundwater Withdrawal Permits; Legal Requirement to Obtain; Naval Installations in the Eastern Virginia Groundwater Management Area* (Feb. 16, 2000) (unpublished manuscript) (on file with the author). *See also* Heather Bloomfield Lee, Note, *Forcing the Federal Hand: Reserved Water Rights v. States' Rights for Instream Protection*, 41 HASTINGS L.J. 1271, 1295 (1990).

¹⁸ Environmental factors account for the difference. As one commenter has noted, the development of the Prior Appropriation Doctrine, a process to determine who is entitled to scarce water resources, "is closely intertwined with the history of the West. The Doctrine is an outgrowth of a principle of mining law, under which the first prospector to stake a claim would be entitled to work that claim." William A. Wilcox & Captain David Stanton, *Maintaining Federal Water Rights in the Western United States*, ARMY LAW., Oct. 1996, at 3, 3. Thus, even non-riparian landowners could acquire water rights by diverting and carrying water to their lands. Some states, like California (hence the name "California" rule), are hybrids, whose legal systems include both riparian and appropriative rights. *See* *Irwin v. Phillips*, 5 Cal. 140 (1855); *In re Water of Hallett Creek Stream System*, 749 P.2d 324 (Cal. 1988) (upholding the United States Forest Service's state-law based claim of riparian rights on reserved Federal lands).

1. Common Law Riparian Rights

Most eastern states have adopted, with some variation and modification, the common law riparian theory of water rights. In general, under a riparian theory, the right to use water is a property right running appurtenant to the ownership of land.

The riparian water right does not depend on actual use of the water—it exists whether or not the landowner in fact uses the water.¹⁹ Under the riparian doctrine, property owners are entitled to the reasonable use of streams and bodies of water.²⁰ Distinguishing between “natural” and “artificial” uses, riparian landowners may divert as much water as necessary for “natural” uses (e.g., bathing, drinking, household purposes) but may only divert water for artificial uses (e.g., irrigation, manufacturing, power generation, mining) as long as such uses do not materially interfere with the natural flow of the watercourse.²¹

2. Common Law Appropriative Rights

In response to water scarcity due to arid and semi-arid conditions, the western states developed and eventually codified as part of their statutory laws what has come to be known as the “law of the first taker” or the “appropriative” system.²² This system was based on the customs and traditions of western mining camps prior to the establishment of formal state or territorial governments.²³ Under an appropriative system, unlike a riparian system, the right to use water does not depend on ownership of underlying or appurtenant

¹⁹ Michael G. Proctor, *Section 10 of the Rivers and Harbors Act and Western Water Allocations—Are the Western States Up a Creek Without a Permit?* 10 B.C. ENVTL. AFF. L. REV. 111, 116 n.32 (1982) (citing ROBERT E. BECK & C. PETER GOPLERUD, 7 WATERS AND WATER RIGHTS, VOL. 3, 309-10 (R. Clark ed., The Allen Smith Co. 1967 & Supp. 1978)).

²⁰ Anita Porte Robb, *Applying the Reserved Rights Doctrine in Riparian States*, N.C. CENT. L. J. 98-99 (1983).

²¹ Richard C. Ausness, *Water Rights, the Public Trust Doctrine, and Protection of Instream Uses*, 1986 U. ILL. L. REV. 407, 416 n.75 (1986) [hereinafter Ausness, *Water Rights—Protection of Instream Uses*] (citing Eva Morreal Hanks, *The Law of Water in New Jersey*, 22 RUTGERS L. REV. 621, 628-29 (1968)).

²² DoJ Memo, *supra* note 5, at 8. See also Bell & Johnson, *supra* note 10, at 23. The western states using this doctrine are: Arizona, California, Colorado, Idaho, Kansas, Montana, Nebraska, Nevada, New Mexico, North Dakota, Oklahoma, Oregon, South Dakota, Texas, Utah, Washington, and Wyoming.

²³ *Id.*

lands; rather, the right depends on the appropriation of the water for a particular use.²⁴

The appropriative rights doctrine incorporates a “first in time, first in right” theory to consumptive water use.²⁵ Promoting the investment of capital necessary to develop western water supplies, the first water user to divert water from any watercourse and put it to beneficial use acquires a right that is superior to that of any subsequent user.²⁶ In cases of insufficient water, priority is chronological—the first user gets the water, rather than prorating among competing potential users.²⁷ In other words, the first person to put the water to beneficial use is entitled to that water as long as the use continues, to the exclusion of subsequent users.

Appropriative rights are not restricted to riparian owners and are perpetual in duration.²⁸ To affirmatively claim a right, appropriators must appropriate and use a definite quantity of water, usually expressed in terms of cubic feet per second in the case of direct diversions or in terms of acre-feet for reservoir storage.²⁹ Once vested, the appropriated water right becomes a protected property interest, which can be sold, leased, or otherwise alienated, provided the water use is continued.³⁰

The underlying prerequisite to an appropriative water right is that the water must be physically diverted³¹ and put to a publicly defined beneficial use.³² Beneficial use is defined as any use of water that is reasonable, useful, and beneficial to the appropriator and is, at the same time, consistent with the public’s interest in the best utilization of water supplies.³³ Absent an actual application of water to a beneficial use, there is no valid appropriation. The

²⁴ *Id.*

²⁵ See Ausness, *Water Rights—Protection of Instream Uses*, *supra* note 21, 416 n.75.

²⁶ *Id.*

²⁷ Wilcox & Stanton, *supra* note 18, at 3.

²⁸ *Id.*

²⁹ *Id.*

³⁰ Steven E. Clyde, *Adapting to the Changing Demand for Water Use Through Continued Refinement of the Prior Appropriation Doctrine: An Alternative Approach to Wholesale Reallocation*, 29 NAT. RESOURCES J. 435, 436 (1989).

³¹ See Mary Ann King, *Getting Our Feet Wet: An Introduction to Water Trusts*, 28 HARV. ENVTL. L. REV. 495, 500 (2004) (noting that historically, beneficial use referred to physical diversion of water for consumptive or out-of-stream agricultural, domestic, and mining uses and did not include habitat and species protection or instream flows).

³² Bell & Johnson, *supra* note 10, at 5.

³³ Proctor, *supra* note 8, at 116–17 n.41 (citing *Tulare Irr. Dist., v. Lindsey-Strathmore Irr. Dist.*, 45 P.2d 972, 1007 (Cal. 1935); *Finney County Water Users’ Ass’n v. Graham Ditch Co.*, 1 F.2d 650, 652 (D. Colo. 1924)).

beneficial use is also the measure of the right; an appropriator is entitled to only that quantity of water beneficially used in any given year upon particular land.³⁴

In order to preclude speculative claims and assure protection of the public interest in the continuous beneficial use of water, the appropriative right doctrine penalizes nonuse by forfeiture.³⁵ Water relinquished by nonuse is returned to the water system and is available for appropriation by others.³⁶

3. Common Law Groundwater Rights

The common law classifies groundwater as either underground streams or percolating waters, and different rules apply to each category.³⁷ Underground streams flow in well-defined channels below the earth's surface, generally have ascertainable banks and courses, and are subject to the same rules that govern surface watercourses.³⁸ Such streams are, however, relatively uncommon.³⁹

More prevalent are percolating waters which have no defined channel but rather seep or filter through the soil beneath the ground's surface.⁴⁰ These waters have unknown courses and are not discoverable from surface indications.⁴¹ Rights to percolating groundwater are distinguishable from riparian rights governing surface waters and underground streams. Rights to percolating groundwater are not riparian; rather they arise from ownership of property that overlies groundwater.⁴² Although the use rules of percolating groundwater are fragmented and confusing, three major approaches in the eastern United States are discernible: (1) the English, or absolute ownership doctrine; (2) the American, or reasonable use rule; and (3) the correlative rights doctrine. The English, or absolute ownership rule, allows a landowner to extract an unlimited quantity of percolating water groundwater from his land and use it on either overlying or distant lands regardless of injury to adjoining landowners.⁴³ The rule prohibits only waste or malicious injury.⁴⁴ Under the

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

³⁷ Richard C. Ausness, *Water Rights Legislation in the East: A Program for Reform*, 24 WM. & MARY L. REV. 547, 550 (1983) [hereinafter Ausness, *Water Rights—A Program for Reform*].

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.* at 550–51 (citing *Clinchfield Coal Corp. v. Compton*, 139 S.E. 308, 311 (Va. 1927)).

⁴¹ Ausness, *Water Rights—A Program for Reform*, *supra* note 37, at 550

⁴² Parsons, *supra* note 17, at 3 n.7 (citing A. DAN TARLOCK, *LAW OF WATER RIGHTS AND RESOURCES* 4-2 to 4-4.1, 4-17 (1999)).

⁴³ According to the English, or absolute ownership, rule, a landowner may extract an unlimited quantity of percolating groundwater from his or her land and use it on either overlying or distant lands regardless of injury to adjacent landowners. *Stone v. Pattern*, 63 S.E. 897 (Ga. 1909); *Edwards*

American, or reasonable use rule, a landowner may use as much percolating groundwater as needed for uses reasonably related to the natural uses of the overlying land, regardless of adverse effects on adjacent landowners.⁴⁵ Encompassing most agricultural, domestic, mining, and manufacturing uses, the water use must be beneficial.⁴⁶ According to the correlative rights doctrine, landowners sharing a common groundwater pool each have an equal and correlative right to use the water to benefit their overlying lands.⁴⁷ In times of shortage, each overlying landowner is entitled to an apportioned equitable share of the groundwater.⁴⁸

4. State Statutory Water Allocation Regimes

Today, the common law has been supplemented or preempted by some form of codified statutory water allocation system and all potential appropriators must apply to their states for permission to appropriate water, usually from a water program agency.⁴⁹ In the East, some of the states expressly incorporate the beneficial use standard in their water rights legislation,⁵⁰ while others⁵¹ do so implicitly.⁵²

v. Haeger, 54 N.E. 176 (Ill. 1899). This rule imposes liability only for waste or malicious injury to another. *Wheatley v. Baugh*, 25 Pa. 528 (1855). See Ausness, *Water Rights—A Program for Reform*, *supra* note 37, at 551 n.17 (citing *Stone*, 63 S.E. at 897; *Edwards*, 54 N.E. at 176).

⁴⁴ Ausness, *Water Rights—A Program for Reform*, *supra* note 37, at 551 n.18, (citing *Roath v. Driscoll*, 20 Conn. 533 (1850); *St. Amand v. Lehman*, 47 S.E. 949 (Ga. 1904); *Gagnon v. French Lick Springs Hotel Co.*, 72 N.E. 849 (Ind. 1904); *Greenleaf v. Francis*, 35 Mass. (18 Pick.) 117 (1836); *Wheatley*, 25 Pa. at 528).

⁴⁵ The American, or reasonable use, rule allows a landowner to use as much percolating groundwater as he or she needs, regardless of adverse effects on other landowners, if the use is reasonably related to the natural uses of the overlying land. Ausness, *Water Rights—A Program for Reform*, *supra* note 37, at 551. Generally, reasonable uses include most agricultural, domestic, mining, and manufacturing uses. *Drummond v. White Oak Fuel Co.*, 140 S.E. 57 (W. Va. 1927). See Ausness, *Water Rights—A Program for Reform*, *supra* note 37, at 551.

⁴⁶ *Id.*

⁴⁷ The correlative rights doctrine provides that each individual owning land over a common groundwater pool has an equal and correlative right to use the water to benefit his or her overlying land. The doctrine provides that groundwater be apportioned equitably among overlying owners in times of shortage and that each owner is entitled to no more than a fair and just proportion of the water. Ausness, *Water Rights—A Program for Reform*, *supra* note 37, at 552.

⁴⁸ *Id.*

⁴⁹ Proctor, *supra* note 8, at 118.

⁵⁰ See, e.g., VA. CODE ANN. § 62.1-255 (2014).

⁵¹ See, e.g., MD. CODE ANN., ENVIR. § 5-501(a) (LexisNexis 2014) ["In order to conserve, protect, and use water resources of the State in accordance with the best interests of the people of Maryland, it is the policy of the State to control, so far as feasible, appropriation or use of surface waters and groundwaters of the State."]

⁵² Memorandum from LT Paul Ziegler, JAGC, USN, to CDR (Sel) Michael Palmer, JAGC, USN, subject: Groundwater Law and Withdrawal Compliance 2 (15 Dec. 2000) (copy on file with author);

Most of the western states have adopted statutory permit systems for recognition, administration, and enforcement of water rights based primarily on the common law appropriation doctrine.⁵³ As with the eastern statutory regimes, all potential appropriators must apply for and obtain a permit from the state or local municipality to secure water rights. Under a typical statutory permit system adopted by the western states, a public record typically exists, identifying the date when an application was initiated and the scope of the requested right.⁵⁴ Significantly, however, it is well recognized that the approval of a new application for water rights under a statutory permit system cannot impair a previously vested right to water.⁵⁵ Moreover, most of the western states, either by statute or judicial decision, prohibit the recognition of new water rights under a statutory permit system when a stream is fully appropriated.⁵⁶ Indeed, there are state statutes that expressly authorize the government to purchase water from persons who have acquired vested rights in order to preserve the natural stream flow of a river.⁵⁷

D. Federal Water Rights Doctrines

Unless the Federal Government, as a water user, can assert limited federal water rights, it must navigate the state regimes discussed above to acquire needed water. This section discusses the limited federal common law doctrine on Federal Reserved Water Rights and Federal Non-Reserved Water Rights which developed in response to the applicability of the above-discussed state water allocation regimes to federal agencies.

see also, DoJ Memo, *supra* note 5, at 8 n.6 (citing Frank J. Trelease, *Government Ownership and Trusteeship of Water*, 45 CALIF. L. REV. 638, 641 n.12 (1957)).

⁵³ For example, Oregon enacted a water rights statute in 1909 declaring future water rights based on state law could only be acquired through a permit system enacted by the state legislature. OR. REV. STAT. § 539.010 (1909). *See* United States v. Oregon, 44 F.3d 758, 764 (9th Cir. 1994); OR. REV. STAT. ch. 537 (2015) (stating the current codification of statutory permits system). The Oregon statutory scheme provides that those claimants who were issued “water certificates” through the permit system were not required to participate in a general stream adjudication in order to preserve their rights. This statutory permit system adopted by Oregon subsequently served as a model for statutes governing water law that were enacted in Arizona, California, Nevada, and Texas. United States v. Oregon, 44 F.3d at 765. With the exception of Colorado, all of the western states have a formal statutory permit system in place for appropriating waters. *See* 2 ROBERT E. BECK, *WATERS AND WATER RIGHTS* §14.01 (1967).

⁵⁴ BECK, *supra* note 53 at §14.01.

⁵⁵ *See id.* § 14.03(c)(2).

⁵⁶ *See id.* § 14.03(1).

⁵⁷ *Id.*; *see, e.g.*, COLO. REV. STAT. § 37-92-102(3) (2014).

1. Federal Reserved Water Rights

Based on federal proprietary interests and federal constitutional powers, the Federal Reserved Water Rights (reserved water rights) doctrine is a creature of federal common law.⁵⁸ The reserved water rights doctrine provides that when the United States sets aside a federal reservation from public land holdings at large, the amount of water necessary for the primary purposes of the reservation is impliedly reserved for use on the reservation.⁵⁹ In general, federal reserved lands are lands that were never in state or private ownership while acquired lands are those granted or sold to the United States by a state or citizen.⁶⁰ Reserved lands include “national forests, tribal lands embraced within Indian reservations, military reservations, and other lands and interests in lands owned by the United States, and withdrawn, reserved, or withheld from private appropriation and disposal under the public land laws.”⁶¹ Under the reserved water rights doctrine, when the Federal Government withdraws its land from the public domain and reserves it for a particular federal purpose (such as the establishment of a national park, national forest, Indian reservation, or military facility),⁶² the government, by implication, reserves appurtenant water then unappropriated to the extent needed to accomplish the purpose of the reservation.⁶³

The Federal Government has a reserved water right on reserved land only if the United States intended to reserve unappropriated, available water.⁶⁴ This intent is inferred if the previously unappropriated waters are necessary to accomplish the purposes for which the reservation was created.⁶⁵

The U.S. Supreme Court laid the groundwork for the reserved water rights doctrine in the case of *United States v. Rio Grande Dam & Irrigation*

⁵⁸ Bell & Johnson, *supra* note 10, at 49.

⁵⁹ Bell & Johnson, *supra* note 10, at 50; *see* *United States v. New Mexico*, 438 U.S. 696, 699–700 (1978); *Cappaert v. United States*, 426 U.S. 128, 135 (1976).

⁶⁰ *Wallis v. Pan Amer. Petrol. Corp.*, 384 U.S. 63, 65 n.2 (1966).

⁶¹ 16 U.S.C. § 796(2) (2015).

⁶² This reservation may be accomplished by statute, executive order, or treaty. *Federal Power Comm'n v. Oregon*, 349 U.S. 435, 443–44 (1955).

⁶³ *See* *United States v. New Mexico*, 438 U.S. at 700; *Cappaert*, 426 U.S. at 138, 143; *Arizona v. California*, 373 U.S. 546, 595–601 (1963); *United States v. Dist. Ct. for Eagle County*, 401 U.S. 520, 522–23 (1971); *Colo. River Water Conservation Dist. v. United States*, 424 U.S. 800, 805 (1976); *Fed. Power Comm'n v. Oregon*, 349 U.S. 435 (1955); *United States v. Powers*, 305 U.S. 527 (1939); *Winters v. United States*, 207 U.S. 564 (1908).

⁶⁴ *See* *United States v. New Mexico*, 438 U.S. 696 (1978); *Cappaert*, 426 U.S. 128.

⁶⁵ *See, e.g.,* *United States v. New Mexico*, 438 U.S. at 700; *Cappaert*, 426 U.S. at 139; *Arizona v. California*, 373 U.S. at 599–601; *Winters*, 207 U.S. at 576.

Co.⁶⁶ The issue was whether a state could authorize an irrigation company to divert water in a manner that disrupted the navigability of a waterway.⁶⁷ Asserting that the Federal Government's superior power to regulate navigable waterways limits the reach of state water law, the *Rio Grande* Court held that the Federal Government reserved an adequate flow of water for the beneficial use of federal property.⁶⁸ While the decision did not create or recognize, specifically, the reserved water rights doctrine, it did acknowledge for the first time that the Federal Government had the authority to reserve water.

The U.S. Supreme Court first recognized the reserved water rights doctrine in *Winters v. United States*.⁶⁹ In *Winters*, the Supreme Court held that the Federal Government has the authority to claim water rights apart from state law for lands withdrawn from the public domain and that those rights are implicitly reserved.⁷⁰

The Supreme Court officially extended the Winters Doctrine of reserved water rights to non-Indian reservation federal lands in *Arizona v. California*.⁷¹ Intervening in a dispute between Arizona and California over water rights to the Colorado River, the United States asserted reserved water rights for several national forests, national recreation areas, and national wildlife refuges.⁷² Citing the Property and Commerce Clauses of the United States Constitution, the Court held that there was "no doubt about the powers of the United States . . . to reserve water rights for its reservations and its property."⁷³

In *Cappaert v. United States*, the Supreme Court upheld the United States' claim to a federally reserved water right at a pool of water located in an underground limestone cavern at Devil's Hole National Monument for the

⁶⁶ *United States v. Rio Grande Dam & Irrigation Co.*, 174 U.S. 690, 703 (1899).

⁶⁷ *Id.*

⁶⁸ In dictum, the Court stated: "in the absence of specific authority from congress, a state cannot, by its legislation, destroy the right of the United States, as the owner of lands bordering on a stream, to the continued flow of its waters, so far, at least, as may be necessary for the beneficial uses of the government property" *Id.*

⁶⁹ *Winters v. United States*, 207 U.S. 564 (1908).

⁷⁰ *Id.* at 576–77 ("[T]he power of the [Federal] [G]overnment to reserve the waters and exempt them from appropriation under the state laws is not denied, and could not be."); *id.* at 577 (citing *United States v. Rio Grande Dam & Irrigation Co.*, 174 U.S. 690, 702–03 (1899)); *see also* *United States v. Winans*, 198 U.S. 371 (1905).

⁷¹ *Arizona v. California*, 373 U.S. 546 (1963).

⁷² *Id.*

⁷³ *See id.* at 598.

protection of a rare species of fish.⁷⁴ In so doing, the Court set forth a concise statement of the Federal Reserved Water Rights doctrine:

[W]hen the federal Government withdraws its land from the public domain and reserves it for a federal purpose, the Government, by implication, reserves appurtenant water then unappropriated to the extent needed to accomplish the purpose of the reservation. In so doing, the United States acquires a reserved right in unappropriated water that vested on the date of the reservation and is superior to the rights of future appropriators. Reservation of water rights is empowered by the Commerce Clause, which permits regulation of navigable streams, and the Property Clause, which permits federal regulation of federal lands. The doctrine applies to Indian reservations and other federal enclaves, encompassing water rights in navigable and non-navigable streams.⁷⁵

The *Cappaert* Court provided the following three elements of the reserved water rights doctrine: (1) there must be a reservation of federal land, defined as a withdrawal of land from the public domain; (2) the withdrawal must be reserved for a specified purpose; and (3) the federally created reserve is entitled to an implied water right “to the extent needed to accomplish the purposes of the reservation.”⁷⁶

In 1978, in *United States v. New Mexico*, the Supreme Court placed an important limitation on the implied-reservation-of-rights doctrine: Federal Reserved Water Rights serve only the *primary purpose* for which the federal lands are used, and not any secondary purposes.⁷⁷ Rejecting the Federal Government's expansive claim of reserved rights, the Supreme Court refused to extend reserved rights to in-stream flows on national forest lands for recreation, aesthetic, and wildlife purposes.⁷⁸ Instead, the Court limited Federal Reserved Water Rights to only the two primary purposes expressly set forth by the

⁷⁴ *Cappaert v. United States*, 426 U.S. 128 (1976) (groundwater characterized as surface water).

⁷⁵ *Id.* at 138 (internal citations omitted); see also 4 BECK, *supra* note 53, § 37.02(d) (“Reserved waters are . . . not ‘appurtenant’ to land reservations, in the sense of physical attachment, but extend to all waters reasonably necessary to fulfill the reservation purpose.”).

⁷⁶ *Cappaert*, 426 U.S. at 138.

⁷⁷ *United States v. New Mexico*, 438 U.S. 696 (1978). The *New Mexico* case arose from a McCarran Amendment adjudication. “Primary purpose” should be distinguished from similar sounding, but conceptually different, terms, such as “mission essential.” A certain land use may not be mission essential in the broader context of agency mission, and yet it may be a primary purpose for which Congress authorized the land to be purchased. Parsons, *supra* note 17.

⁷⁸ *United States v. New Mexico*, 438 U.S. at 718.

Organic Act of 1897, the act that created the national forests.⁷⁹ These two purposes were to secure “favorable conditions for water flows” and to “furnish a continuous supply of timber for the use and necessities” of the people.⁸⁰ The Supreme Court reiterated that Congress reserved “only that amount of water necessary to fulfill the purpose of the reservation, no more.”⁸¹

Writing for the majority, Justice Rehnquist stated:

Each time this Court has applied the ‘implied-reservation-of-water-doctrine,’ it has carefully examined both the asserted water right and the specific purposes for which the land was reserved, and concluded that without the water the purposes of the reservation would be entirely defeated. This careful examination is required both because the reservation is implied, rather than expressed, and because of the history of congressional intent in the field of federal-state jurisdiction with respect to allocation of water.⁸²

Accordingly, when assessing reserved water rights, the examination focuses on both the “reservation” and the specific “purpose” for which the land was reserved.⁸³

The *New Mexico* case illustrates that the “reservation” and “purpose” for the land will determine the scope of the water right.⁸⁴ In determining the primary purposes of the congressional reservation, the Supreme Court will recognize reserved water rights only upon concluding that “without the water the purposes of the reservation would be entirely defeated.”⁸⁵

Little case law exists regarding reserved water rights on DoD installations. An 1899 Supreme Court decision, *United States v. Krall*,⁸⁶ held that Nevada state law did not control the DoD’s use of groundwater at an ammunition depot.⁸⁷ In *Krall*, a stream was diverted to an Army post for “all

⁷⁹ *Id.*

⁸⁰ *Id.*; see also Bell & Johnson, *supra* note 10, at 59.

⁸¹ *United States v. New Mexico*, 438 U.S. at 700. The Court first pronounced this limitation on the scope of reserved rights in *Cappaert*, 426 U.S. at 141.

⁸² *United States v. New Mexico*, 438 U.S. at 700.

⁸³ *Id.*

⁸⁴ *Id.* at 700.

⁸⁵ *Id.*

⁸⁶ 174 U.S. 385 (1899).

⁸⁷ *Parsons*, *supra* note 17, at 8 n.53 (citing *Nevada ex rel. Shamberger v. United States*, 165 F. Supp. 600 (D. Nev. 1958), *aff’d on other grounds*, 279 F.2d 699 (9th Cir. 1960)).

agricultural, domestic, and practical purposes.”⁸⁸ Although the case was dismissed on procedural grounds, the Court did not take issue with the broadly stated purpose for the water need.

In *United States v. District Court In & For Water Division No. 5*, the Supreme Court, while noting *in dicta* “[T]he Department of the Navy administers certain naval petroleum and oil shale reserves which, if ever developed, would require water to accomplish the federal purpose for which the reservations were made,” held the Colorado state court had jurisdiction to adjudicate the reserved water rights of the United States pursuant to 43 U.S.C. § 666.⁸⁹

For DoD installations, the burden is on DoD to examine the original reservation or acquisition to determine the military reservation’s primary purpose(s) and to demonstrate that the quantities claimed are necessary to fulfill the purpose. While DoD is entitled to significant executive discretion in determining the primacy of its installations’ and activities’ purposes, the federal courts will likely be the final arbiters of the “primary/secondary” purposes. What is clear is that an installation commander’s mere declaration of “primary” purpose will, in and of itself, be insufficient. Thus, land reserved from the public domain for a “defense base” has Federal Reserved Water Rights for some, but not all, activities necessary to the operation of the installation. While it is still an open question as to what constitutes “secondary” purposes, it appears that Federal Reserved Water Rights may not be available at defense installations for purposes such as water used for conservation and land management, wildlife enhancement, in-stream flow maintenance, farming or other uses on out-leased lands, recreation, and water sold for purposes not related to installation needs. These other purpose water uses independent of the congressional reservation must be acquired under applicable state law or through specific legislation.⁹⁰

⁸⁸ *Krall*, 174 U.S. at 385–86.

⁸⁹ *United States v. Dist. Ct. In & For Water Div. No. 5*, 401 U.S. 527, 530 (1971).

⁹⁰ *United States v. New Mexico*, 438 U.S. at 701–03 (“Where Congress has expressly addressed the question of whether federal entities must abide by state water law, it has almost invariably deferred to the state law. Where water is necessary to fulfill the very purposes for which a federal reservation was created, it is reasonable to conclude, even in the face of Congress’ express deference to state water law in other areas, that the United States intended to reserve the necessary water. Where water is only valuable for a secondary use of the reservation, however, there arises the contrary inference that Congress intended, consistent with its other views, that the United States would acquire water in the same manner as any other public or private appropriator.”) (citations omitted); *see* BECK, *supra* note 53, § 37.06.

While the *New Mexico* decision benefits federal agencies by endorsing Federal Reserved Water Rights for uses that further the “primary” purpose of the federal reservation, it strangely fails to address the requirement for a valid waiver of federal sovereignty to justify its finding that other federal appropriations must be acquired under applicable state law. In fact, in none of the cases referenced above does the Court analyze the federal sovereignty issue and instead glosses over the question by citing to prior pronouncement of general Congressional deferral to state law when it comes to water allocation. Today, it is difficult to see how the Court would reach the same conclusion of presumed state authority to regulate federal agency activities that it reached in its 1978 *New Mexico* decision applying the enhanced Congressional sovereign immunity waiver standards set forth in its 1992 *U.S. Dep’t of Energy v. Ohio* decision. Federal sovereign immunity is discussed further later in Part I.

2. Federal Non-Reserved Water Rights

Another potential source of federal water rights is federal non-reserved water rights. Under the non-reserved water rights doctrine, the Federal Government has a right to unappropriated water on federal lands premised in part on the assumption that the United States acquired proprietary rights to all unappropriated water on public lands at the time it acquired the territories that became the western states, and that it has never subsequently granted away that proprietary interest except to the extent that private individuals may have actually appropriated water on those lands.⁹¹ The Supreme Court has characterized the Federal Government’s control over the use and disposition of its property as “complete” and “without limitation,” and has stated that an interest in property of the United States may be acquired only by an express grant from Congress.⁹² Therefore, if the federal agency “owns” the water all that is necessary to perfect its rights is use of that water for an authorized federal purpose.⁹³ The policy is premised on the idea that absent an explicit congressional grant of an ownership interest to the states, a state cannot impose any restrictions on federal agency use of federal lands, including water diversions and groundwater withdrawals.⁹⁴

⁹¹ DOJ Memo, *supra* note 5, at 51.

⁹² See *id.* at 51–52 (citing Federal Water Rights of the National Park Service, Fish, and Wildlife Service, Bureau of Reclamation, and Bureau of Land Management, 86 Interior Dec. 553, 563 (Dep’t of Interior July 25, 1979); see also *Kleppe v. New Mexico*, 426 U.S. 529, 539–40 (1976); *Caldwell v. United States*, 250 U.S. 14, 20–21 (1918).

⁹³ DOJ Memo, *supra* note 5, at 52 (citing Comment, *Federal Non-Reserved Water Rights*, 15 LAND & WATER L. REV. 67, 76 (1980)).

⁹⁴ DOJ Memo, *supra* note 5, at 53.

Some states, however, assert that the Federal Government never acquired ownership of those waters together with the public lands and, even if it did, the Federal Government ceded its ownership interests in the water to the states by the acts of admission into the Union.⁹⁵ The contention is that the state therefore won those waters and can exercise control over their use, even if the use is by the Federal Government.⁹⁶ The only exception to that control is if Congress withdraws land (and water) from the applicability of those acts by a formal reservation.⁹⁷ As discussed above, federal agency claims of “title” to, or “ownership” of, unappropriated water generally do not provide an adequate basis for either the denial or assertion of federal water rights.

Federal reserved water rights can be relied upon on DoD reserved land to the extent the water serves the primary purpose for which the land was reserved. Federal-non-reserved water rights may provide DoD installations a potential additional source of water rights, but this doctrine has not been thoroughly tested and accepted by either Congress or the federal courts. As such, non-reserved water rights could not reasonably be relied on by DoD installations to ensure their access to mission-required water quantities. Accordingly, many DoD installations cannot rely upon federal water rights to meet mission demands and turn, instead, to state regulatory programs to acquire needed water. That solution is problematic for various reasons, but particularly because, to date, the Federal Government has not waived federal sovereign immunity with respect to water acquisition and use.

E. Federal Sovereignty

Under the Supremacy Clause of the U.S. Constitution, federal law is the supreme law of the land.⁹⁸ The Supremacy Clause provides:

[T]his Constitution and the Laws of the United States which shall be made in Pursuance thereof . . . shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any state to the Contrary notwithstanding.⁹⁹

⁹⁵ See *id.* at 51.

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ U.S. CONST. art. VI, cl. 2.

⁹⁹ *Id.*

Accordingly, under the federal supremacy doctrines, the United States enjoys traditional freedom from state and local control.¹⁰⁰

Related to, and flowing from, federal supremacy is the federal common law doctrine of sovereign immunity. The doctrine of federal sovereign immunity bars suits by states and state agencies against the Federal Government, unless the United States has consented to be sued.¹⁰¹ “The United States, as sovereign, is immune from suit save as it consents to be sued” and “[a] waiver of sovereign immunity ‘cannot be implied but must be unequivocally expressed.’”¹⁰² Consequently, the activities of the Federal Government are generally free from regulation by any state and states may not impose penalties or permit requirements on federal facilities without a clear and unambiguous showing of congressional intent to waive sovereign immunity.¹⁰³

Only Congress can waive sovereign immunity, and waivers of sovereign immunity must be unequivocally expressed in statutory text; they may not be implied or inferred but instead must be “surrendered in unmistakable terms.”¹⁰⁴ Since any waiver must be clearly mandated in the Congressional text, legislative history cannot be used to clarify an ambiguity.¹⁰⁵ Thus, waivers are construed strictly in favor of the sovereign.¹⁰⁶ Even where there are compelling policy reasons for a broader waiver, courts must strictly construe the text in favor of the United States and should not infer waiver where Congress has not expressly provided one.¹⁰⁷

¹⁰⁰ See generally *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316 (1819) (national bank not subject to state regulation). As the *McCulloch* Court observed, “[i]t is of the very essence of supremacy, to remove all obstacles to its action within its own sphere, and so to modify every power vested in subordinate governments, as to exempt its own operations from their own influence.” *Id.* at 427.

¹⁰¹ See, e.g., *Block v. North Dakota*, 461 U.S. 273, 280 (1983); *United States v. Testan*, 424 U.S. 392 (1976).

¹⁰² *United States v. Mitchell*, 445 U.S. 535, 538 (1980) (quoting *United States v. Sherwood*, 312 U.S. 584, 586 (1941); *United States v. King*, 395 U.S. 1, 4 (1969)).

¹⁰³ *U.S. Dep’t of Energy v. Ohio*, 503 U.S. 607 (1992); *Hancock v. Train*, 426 U.S. 167, 179 (1976) (holding that under the Clean Air Act, Congress had waived sovereign immunity as to substantive requirements but not procedural requirements); *Mayo v. United States*, 319 U.S. 441, 445 (1943); *Testan*, 424 U.S. 392.

¹⁰⁴ *Bowen v. Pub. Agencies Opposed to Soc. Sec. Entrapment*, 477 U.S. 41, 52 (1986) (quoting *Merrion v. Jicarilla Apache Tribe*, 455 U.S. 130, 148 (1982)). See *U.S. Dep’t of Energy v. Ohio*, 503 U.S. at 619, 627; *United States v. Nordic Vill.*, 503 U.S. 30, 33 (1992); *Block*, 461 U.S. at 287; *Mitchell*, 445 U.S. at 538.

¹⁰⁵ *Nordic Vill.*, 503 U.S. at 37.

¹⁰⁶ *U.S. Dep’t of Energy v. Ohio*, 503 U.S. at 615.

¹⁰⁷ See *Library of Congress v. Shaw*, 478 U.S. 310, 318–21 (1986) (strictly construing the waiver of sovereign immunity to exclude attorney fees from “costs” under the Civil Rights Act of 1964); *Ruckelshaus v. Sierra Club*, 463 U.S. 680, 686 (1983) (holding that waiver of sovereign immunity

Congress has subjected federal agencies to state and local water appropriation and allocation requirements for their acquisition and use activities only once, and for a very limited purpose, through the McCarran Amendment. The McCarran Amendment was enacted by Congress to respond to challenges presented by the Federal Government's refusal to participate in state statutory general stream adjudications.¹⁰⁸ Because of the Federal Government's large landholdings in the west, its claims of sovereign immunity and refusal to participate in these stream adjudications impaired and significantly diminished the value and effectiveness of state water allocation systems.¹⁰⁹ The McCarran Amendment affirmatively waived the Federal Government's sovereign immunity from suit and required its participation in comprehensive general stream adjudications that make "all of the claimants to water rights" parties, resolve disputes between those claimants and establish priorities among the various rights asserted.¹¹⁰ Specifically, it granted express Congressional consent to join the United States as defendant in any suit to adjudicate water rights of all claimants to a particular water course where the United States is owner of or is in process of acquiring such rights, including appropriated rights, riparian rights,

with regard to award of attorney fees under the Clean Air Act should not be enlarged beyond what fair reading of the language requires).

¹⁰⁸ S. REP. NO. 82-755, at 4-6 (1951). The text of the amendment reads as follows:

§ 666. Suits for adjudication of water rights

(a) Joinder of United States as defendant; costs. Consent is hereby given to join the United States as a defendant in any suit (1) for the adjudication of rights to the use of water of a river system or other source, or (2) for the administration of such rights, where it appears that the United States is the owner of or is in the process of acquiring water rights by appropriation under State law, by purchase, by exchange, or otherwise, and the United States is a necessary party to such suit. The United States, when a party to any such suit, shall (1) be deemed to have waived any right to plead that the State laws are inapplicable or that the United States is not amenable thereto by reason of its sovereignty, and (2) shall be subject to the judgments, orders, and decrees of the court having jurisdiction, and may obtain review thereof, in the same manner and to the same extent as a private individual under like circumstances: Provided, That no judgment for costs shall be entered against the United States in any such suit.

(b) Service of summons. Summons or other process in any such suit shall be served upon the Attorney General or his designated representative.

(c) Joinder in suits involving use of interstate streams by State. Nothing in this Act shall be construed as authorizing the joinder of the United States in any suit or controversy in the Supreme Court of the United States involving the right of States to the use of the water of any interstate stream.

Pub. L. No. 82-495 § 208(a)-(c), 66 Stat. 549, 560 (codified at 43 U.S.C. § 666 (2015)).

¹⁰⁹ U.S. Dept. of Energy v. Ohio, 503 U.S. at 639; *See* United States v. Oregon, 44 F.3d, 758, 765 (9th Cir. 1994).

¹¹⁰ Dugan v. Rank, 372 U.S. 609, 618-19 (1963).

and reserved rights.¹¹¹ The adjudication, that is, the determination of the relative rights, must be general and encompass all water claimants.¹¹²

It is clear from the cases dealing with the language of the McCarran Amendment that the amendment does no more than create concurrent jurisdiction for the adjudication of water rights.¹¹³ For McCarran purposes, the issue is whether or not a specific stream adjudication conducted pursuant to a state statute is sufficiently “comprehensive” to constitute a waiver of the Federal Government’s sovereign immunity.¹¹⁴ The McCarran waiver does not extend to private suits between the United States and a private party to determine conflicting water rights contentions or limit federal water rights.¹¹⁵ Nor does it displace Federal District Courts’ original jurisdiction of all civil actions commenced by the United States.¹¹⁶ Finally, it neither permits nor prohibits removal of action.¹¹⁷

Aside from the McCarran Amendment, there has been no Congressional unequivocal and unambiguous waiver of sovereign immunity with respect to federal agency water appropriation. Limited solely to state “comprehensive general stream adjudication(s),” the McCarran waiver has no

¹¹¹ *United States v. Dist. Ct. for Eagle County*, 401 U.S. 520, 525 (1971) (articulating that the phrase “rights to the use of water of a river system” is broad enough to embrace waters reserved for use and benefit of federally reserved lands); *see also* *United States v. Dist. Ct., Water Div. No. 5, Colo.*, 401 U.S. 527 (1971) (43 U.S.C. § 666 consent to suit of the United States by provision of the McCarran Amendment extended to reserved rights).

¹¹² *United States v. Hennen*, 300 F. Supp. 256 (D. Nev. 1968).

¹¹³ Senator McCarran himself stated “S. 18 is not intended . . . to be used for any other purpose than to allow the United States to be joined in a suit wherein it is necessary to adjudicate all of the rights of various owners on a given stream. This is so because unless all of the parties owning or in the process of acquiring water rights on a particular stream can be joined as parties defendant, any subsequent decree would be of little value.” S. REP. NO. 82-755, at 9. *See also* *Colo. River Water Conservation Dist. v. United States*, 424 U.S. 800 (1976); *United States v. Dist. Ct. for Eagle County*, 401 U.S. at 525; *Dugan*, 372 U.S. 609; *Nevada ex rel. Shamberger v. United States*, 279 F.2d 699 (9th Cir. 1960); *Hage v. United States*, 35 Fed. Cl. 147 (1996) (holding that the McCarran Amendment does not preclude federal courts from exercising general federal jurisdiction under 28 U.S.C. § 1331 regarding water rights claims and does not limit jurisdiction of Court of Federal Claims to hear water takings claims).

¹¹⁴ *See Dugan*, 372 U.S. at 618–19.

¹¹⁵ *Dugan*, 372 U.S. at 618; *Gardner v. Stager*, 103 F.3d 886 (9th Cir. 1996). *See also* *Lenoir v. Porters Creek Watershed Dist.*, 586 F.2d 1081 (6th Cir. 1978) (holding that 43 U.S.C. § 666 does not constitute a waiver of governmental immunity for private park claim against the United States for flood damage).

¹¹⁶ *Cappaert v. United States*, 426 U.S. 128 (1976). *See* 28 U.S.C. § 1345 (2015) (“United States as plaintiff. Except as otherwise provided by Act of Congress, the district courts shall have original jurisdiction of all civil actions, suits or proceedings commenced by the United States, or by any agency or officer thereof expressly authorized to sue by Act of Congress.”).

¹¹⁷ *Nat’l Audubon Soc’y v. Dep’t of Water & Power*, 496 F. Supp. 499 (E.D. Cal. 1980).

applicability to a federal agency's immunity from a state's operation of a statutory or common law water appropriation or use regime (designed to assign or limit *future* water rights or uses). Accordingly, state and local water allocation requirements cannot lawfully undermine or otherwise invalidate federal agency water acquisition or use. Similarly, state or local appropriation or use laws and regulations, including quantity and use restrictions and registration, permit and fee requirements, cannot be administratively or judicially enforced against federal agencies under the McCarran Amendment waiver of sovereign immunity.¹¹⁸ Absent any other unambiguous Congressional waiver subjecting DoD installations engaged in self-supplied water acquisition and use to state and local water program requirements, these agency activities are immune.¹¹⁹ As such, these same state and local requirements purporting to regulate federal agency self-supplied water acquisition and use are unenforceable against federal agencies and federal agency compliance is not required.

Absent federal Congressional water rights statutory authority and a valid waiver of sovereign immunity subjecting federal agencies to state and local water allocation requirements, the federal courts have been left with the task of attempting to balance Congressionally-articulated general deference to the states when it comes to managing water as a natural resource and the unique status of federal agencies who are immune from state and local regulation and enforcement.

F. Summary

Absent federal law or guidance on water regulation and use, the states developed distinct and comprehensive common law and statutory regimes to regulate water allocation within their borders. This raises unique issues for federal agency landowners who need and use water. Careful analysis reveals no

¹¹⁸ See *Nevada ex rel. Shamberger v. United States*, 279 F.2d 699, 700–01 (9th Cir. 1960) (holding that a state administrative agency's proceeding against the United States was not a general stream adjudication under the McCarran Amendment); *Wyoming v. United States*, 933 F. Supp. 1030 (D. Wyo. 1996) (holding same as above); See also *Miller v. Jennings*, 243 F.2d 157, 159–60 (5th Cir. 1957) (“There can be an adjudication of rights with respect to the upper Rio Grande only in a proceeding where all persons who have rights are before the tribunal.”); *In re Snake River Basin Water System*, 764 P.2d 78, 85 (Idaho 1988) (“[The] history of the McCarran Amendment and the interpretations that the federal courts have given to it convince us that in order for the United States to be subject to the jurisdiction of the trial court in the Snake River basin adjudication, the rights of all claimants on the Snake River and all of its tributaries within the state of Idaho must be included in the adjudication.”).

¹¹⁹ But see DoJ Memo, *supra* note 10, at 79 (assuming federal agencies must acquire water in accordance with state law requirements absent frustration of a specific congressional purpose); Jeremy N. Jungreis, “Permit” Me Another Drink: A Proposal for Safeguarding the Water Rights of Federal Lands in the Regulated Riparian East, 29 HARV. ENVTL. L. REV. 369, 388 n.161 (2005).

valid Congressional waiver of federal sovereignty sufficient to authorize federal agency compliance with state and local water allocation requirements.

Congressional deference to state control and management of water resources and the absence of a sovereign immunity waiver has led the federal courts to develop federal common law water rights doctrines. These doctrines do not satisfactorily resolve the federal agency's water acquisition and use concerns, because not all DoD installations are located on federal reserved land, the Federal Non-Reserved Water Rights doctrine has not been tested for success, and for those installations located on reserved land, the primary and secondary purposes for the reservation do not always yield sufficient water quantities to complete mission requirements.

This lack of sufficient statutory, Executive, agency, and case law guidance leaves individual DoD installation and activity commanders on their own to determine whether to comply with state or local requirements, how to balance the federal and state interests, and whether to accept the risks of succumbing to state regulation or causing or exacerbate Federal-State political tensions and conflict by asserting federal sovereign immunity.

In the absence of a federal statutory or Executive Order fix, the DoD would benefit from regulatory policy guidance that meets Congress's general intent to defer to state and local water allocation regime requirements without compromising federal sovereignty.

II. Meeting Department of Defense Water Needs For National Security— A Proposed Policy

A. Why a DoD Water Rights Policy?

As demonstrated by Part I, the absence of any federal law or directive on federal water rights has led DoD installations to rely on both federal common law and varying state regulatory regimes to acquire and use water. In order to ensure access to sufficient water to meet national security needs, a uniform approach is warranted that addresses this conflict among competing sovereigns; one that allows DoD to obtain the water it needs while respecting sovereign state regulatory interests. The policy must meet three critical imperatives. First, it must be uniform. Second, it must recognize, assert, maintain, and not cede or waive the independent, superior authorities of DoD installations to access and use sufficient water to ensure compliance with their respective current and future national defense missions. Finally and ideally, it must accomplish this access and use by a means that is least disruptive to federal and state relations,

fosters mutual cooperation, and, most importantly, provides appropriate deference to state and local water use requirements and regulatory regimes.

Several policy options are available to DoD. First, the DoD could direct its services to comply with state and local water allocation regime requirements, citing Congress's traditional deference to the states on matters of water allocation¹²⁰ as justification for either full or partial compliance with state and local water allocation program requirements. If DoD formally adopts this course of action, it would merely ratify current practices whereby inconsistent processes are pursued across the services. The common practice is that an installation either completely submits to state and local requirements or the installation achieves partial compliance through a "cafeteria plan" approach in which installations pick and choose the requirements they believe they can and should comply with from the water allocation agencies' compliance requirements menu.

Under this approach, DoD installations are treated no differently than any other landowner in the state and DoD would have to identify, quantify, assert, maintain, and protect DoD's current and reasonably foreseeable state and federal self-supplied water use rights. These water rights would vary depending on how the installation or facility was acquired and whether the installation is located in a riparian, appropriative, or hybrid jurisdiction. This option, of course, would subject DoD installations to all or some state- or local-imposed compliance requirements, fees, and use restrictions. This option does not meet all three imperatives, listed above, because it fails to assert the independent, superior authority of DoD as a federal agency and it does not ensure access to sufficient water to meet DoD mission needs.

Another option available to DoD, one that falls on the other end of the spectrum, is to assert federal sovereignty, declare DoD activities outside the scope of state or local control, ignore state and local water allocation regime requirements, refuse to cooperate with state and local water management programs, and continue groundwater withdrawals or surface water diversions it deems necessary to meet federal mission purposes. The sovereign immunity issue, in this context, has never been challenged, so DoD, through the U.S. Department of Justice, would have to seek a favorable judicial ruling. This option is problematic because it would not meet all three of the imperatives listed above. First, this option would unnecessarily disrupt state and federal relations. Further, it is unclear the U.S. Department of Justice would assert the

¹²⁰ At best, Congress's general deference signals the lack of federal preemption, not valid waivers of federal sovereign immunity.

sovereign immunity defense, or whether the defense would be successful, making this an unreliable long-terms solution.¹²¹

A third option is to seek federal legislative relief. While DoD installations would prefer Congress's unequivocal invocation of full federal sovereignty with accompanying unrestricted federal water rights, the more likely political result would be a codification of the Federal Reserved Water Rights doctrine limiting unrestricted water allocations for primary mission purposes only. Either of these statutory options would meet the three imperatives listed above, however, these are time-consuming solutions to an increasingly urgent problem. Further, the likelihood of success is minimal given the heightened emotional, financial, and political sensitivities surrounding water allocation and management. This is especially true in the American west, where there are deeply held beliefs about the proper role of the federal government when it comes to dictating the proper exercise of an individual's property rights, including one's ability to withdraw and use groundwater or surface water on one's property. Finally, this option is improper because it could expedite depletion of state water resources, the supply of which is in the national interest as it supports agriculture, business, and the national economy. Accordingly, there is no reasonable likelihood Congress has either the desire or will to spend the political capital required to pass and implement a comprehensive federal water use statute that affirmatively asserts federal agency autonomy from state and local water allocation and use requirements. For the same reasons, it is similarly unlikely the President will issue an Executive Order mandating federal agency non-compliance with state water allocation regime requirements.

Finally, the DoD has the option of crafting and implementing agency policy guidance pending Congressional legislation or Presidential Executive Order direction. Rooted in cooperative federalism, this option balances the equally legitimate interests of the federal government sovereignty and state interests in managing and allocating its natural resources. Premised on the federal Coastal Zone Management Act's Federal Consistency requirement, this policy requires DoD installations to comply with state and local water management programs "to the maximum extent practicable." This approach ensures compliance with federal law restrictions on funding and permissible activities, preserves DoD federal agency sovereignty, and reserves final determination of the extent of the installation's cooperative compliance with state and local water allocation requirements to the discretionary authority of the

¹²¹ *Coastal Zone Management Act*, NAT'L OCEANIC AND ATMOSPHERIC ADMIN., <http://coast.noaa.gov/czm/act/> (last visited May 31, 2015); *Federal Consistency Overview*, NAT'L OCEANIC AND ATMOSPHERIC ADMIN., <http://coast.noaa.gov/czm/consistency/> (last visited May 31, 2015).

DoD, not the state or local authorities. This option, proposed by the author and described in more detail below, meets all three of the above imperatives and offers a proven, functional, legally compliant, and politically acceptable interim solution to the current problem pending congressional clarification or direction to the contrary.

B. A Model for DoD: The Federal Coastal Zone Management Act

1. Coastal Zone Management Act (CZMA) Overview

The CZMA,¹²² enacted in 1972 and administered by the U.S. Commerce Department's National Oceanic and Atmospheric Administration's Office of Ocean and Coastal Resource Management, “provides for management of the nation's coastal resources, including the Great Lakes, and balances economic development with environmental conservation.”¹²³ It does so by encouraging “coastal states, Great Lakes states, and United States territories and commonwealths (collectively referred to as coastal states) to develop comprehensive programs to manage and balance competing uses of and impacts to coastal resources.”¹²⁴

2. Coastal Zone Management Act Federal Consistency Requirement

Breaking Congressional precedence with other major federal environmental protections laws, such as the Clean Water Act,¹²⁵ Clean Air Act,¹²⁶ and the Resource Conservation and Recovery Act,¹²⁷ the CZMA does not mandate federal agency compliance with state, territorial, or commonwealth statutory and regulatory requirements. Instead, it emphasizes the primacy of state decision-making regarding the management of coastal uses and resources by putting in a unique “federal consistency” requirement to facilitate federal agency cooperation and coordination with state coastal management programs.¹²⁸ This federal consistency requirement places an affirmative obligation on federal agencies to ensure activities deemed to have reasonably foreseeable effects on any land or water use or natural resource of the coastal zone are “carried out in a manner which is *consistent to the maximum extent*

¹²² Coastal Zone Management Act, 16 U.S.C. §§ 1451-1466 (2015).

¹²³ *Coastal Zone Management Act*, *supra* note 121; *Federal Consistency Overview*, *supra* note 121.

¹²⁴ *Coastal Zone Management Act*, *supra* note 121; *Federal Consistency Overview*, *supra* note 121.

¹²⁵ 33 U.S.C. § 1323(a) (2015).

¹²⁶ 42 U.S.C. § 7418 (2015).

¹²⁷ 42 U.S.C. § 6961 (2015).

¹²⁸ 16 U.S.C. § 1456 (2015).

practicable with the enforceable policies of [federally] approved State management programs.”¹²⁹

For a federal activity to be “consistent to the maximum extent practicable” with a state Coastal Management Program, it must be fully consistent with the enforceable policies of the Program unless federal legal requirements prohibit full consistency.¹³⁰ In other words, if a Federal agency must violate federal law to comply with the enforceable policies, it is not required to do so. Assuming no violation of federal law, federal agency actions must be consistent with applicable enforceable policies.¹³¹

The term “enforceable policy” means “[S]tate policies which are legally binding through constitutional provisions, laws, regulations, land use plans, ordinances, or judicial or administrative decisions, by which a State exerts control over private and public land and water uses and natural resources in the coastal zone,” which are incorporated in a state’s federally approved Coastal Management program.¹³³ Since the CZMA does not authorize the application of enforceable policies to federal agency actions, coastal states apply their enforceable policies through the CZMA federal consistency review process.¹³⁴

The CZMA federal consistency review process requires the federal agency to determine whether coastal effects are reasonably foreseeable results of the proposed agency activity or activities.¹³⁵ If so, the federal agency submits a CZMA Consistency Determination (CD) to the applicable coastal state’s Coastal Management Program at least 90 days before activity starts.¹³⁶ The federal agency’s CD should include a detailed description of the proposed activity, its expected coastal effects, and an evaluation of how the proposed activity is consistent with applicable enforceable policies in the coastal state’s coastal Management Program.¹³⁷

¹²⁹ 16 U.S.C. § 1456(c)(1)(a) (emphasis added).

¹³⁰ *CZMA Federal Consistency Overview: Section 307 of the Coastal Zone Management Act of 1972*, NAT’L OCEANIC AND ATMOSPHERIC ADMIN. 5, 6 (Feb. 20, 2009), http://coastalmanagement.noaa.gov/consistency/media/FC_overview_022009.pdf.

¹³¹ *Id.*

¹³³ 15 C.F.R. § 930.11(h) (2015).

¹³⁴ *CZMA Federal Consistency Overview: Section 307 of the Coastal Zone Management Act of 1972*, *supra* note 130.

¹³⁵ *Id.* at 11.

¹³⁶ *Id.*

¹³⁷ *Id.*; 15 C.F.R. § 930.39 (2015) (content of a consistency determination).

After review and within 60 days, the coastal state either concurs with or objects to the federal agency's consistency determination.¹³⁸ If a coastal state agrees with the federal agency's consistency determination, the agency may proceed with the planned activity.¹³⁹ If the coastal state objects to the federal agency's determination, the state's objection should describe how the proposed activity is inconsistent with specific enforceable policies of the coastal state's Coastal Management Program and the coastal state and federal agency should attempt to resolve their differences.¹⁴⁰ If the conflict or conflicts cannot be resolved, the federal agency can postpone the activity or, notwithstanding coastal state objection, proceed with the proposed agency activity if the Federal agency clearly describes, in writing, to the coastal state how the activity is consistent to the maximum extent practicable.¹⁴¹ Thus, "a Federal agency may proceed with an activity over a state's objection if the Federal agency determines its activity is consistent to the maximum extent practicable with the enforceable policies of the state's [Coastal Management Program]."¹⁴²

3. Applying Federal Consistency to Water Resources Allocations

As demonstrated above, the CZMA's federal consistency requirement provides DoD a proven, functional model of a statutory scheme, short of wholesale waiver of federal sovereignty, which requires the fullest extent of legally permissible federal agency cooperation and coordination with coastal state management program requirements. What works to the mutual benefit of federal and state interests for the preservation and protection of coastal resources and uses should also work to the mutual benefit of federal and state interests for the preservation and protection of water allocations and uses.

C. A Proposed DoD Water Rights Policy

This section provides a summary outline of a proposed federal consistency-based DoD policy. A complete copy of the proposed policy is appended to this article.

¹³⁸ CZMA Federal Consistency Overview: Section 307 of the Coastal Zone Management Act of 1972, *supra* note 130, at 11.

¹³⁹ *Id.* at 12.

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.*

1. Scope and Applicability

The proposed policy identifies requirements, establishes policy, and assigns responsibilities for the use, protection, documentation, and assertion of water use activities by DoD installations located in the United States and its territories and commonwealths. The term “water use activities” is defined as any self-supplied water appropriation, acquisition, and use, including, but not limited to, ground water withdrawals and surface water diversions, performed by or on behalf of a DoD installation. It includes a wide range of installation practices related to, and reasonably likely to affect, water withdrawals or uses (e.g., digging wells) but expressly does not apply to activities related to water supplied to DoD installations or tenants from sources off the installation pursuant to contracts with municipalities or other water suppliers.

2. Policy

The proposed policy asserts DoD shall assert, maintain, and protect all installation water use activities on federal lands, however acquired, where present and reasonably foreseeable water needs are necessary for accomplishment of its statutory national defense missions. This includes assertion of federal sovereignty from state and local water program requirements and controls. To ensure compliance with Federal Anti-Deficiency Act¹⁴³ and other fiscal limitations, DoD installations shall not comply with any state or local water program requirements, including, but not limited to permitting and registration, inspections, fees, water use prohibitions or restrictions, or other similar requirements pertaining to the installations self-supplied water appropriations, acquisitions, or uses unless required by federal law and allowed by the Comptroller General of the United States.

These prohibitions, however, do not restrict DoD, as a matter of comity, from adopting and implementing a policy mandating installation cooperation and coordination with state and local water programs¹⁴⁴ on matters related to the installation's relevant water use activities. Thus, the fundamental philosophy of the proposed DoD policy is an affirmative, voluntarily adopted obligation by DoD directing its installation and activity commanders to coordinate and cooperate with state and local water program requirements to the fullest extent possible without conceding federal sovereignty. The mechanism to

¹⁴³ 31 U.S.C. § 1341 (2015).

¹⁴⁴ Water Allocation Management Programs. Those laws and regulations adopted by a state, territory, commonwealth, or political sub-division thereof for the allocation, management, or conservation of water. It includes local and regional water authorities. *See* Appendix, Dep’t of Defense Federal Water Use Activities ¶ 2.9, *infra*.

strike the balance between protecting federal sovereignty and respecting state and local rights and interests is the adoption of CZMA's Federal Consistency model, which requires federal agency coordination, cooperation, and good faith efforts to comply with applicable state coastal resource and use management policies.¹⁴⁵

3. DoD Installation Water Use Activity Federal Consistency Process Overview

The proposed policy requires, in those circumstances where DoD installation compliance with state or local water program requirements are not authorized under federal law, installation water use activities shall be consistent to the maximum extent practicable with the enforceable policies of the applicable water program.

The term "enforceable policy" means water program policies legally binding through constitutional provisions, laws, regulations, land use plans, ordinances, or judicial or administrative decisions, by which a water program exerts control over private and public water allocations, acquisitions, and uses and which are expressly incorporated in the applicable water program. In most circumstances, these policies are found in the applicable water management program's authorizing statute and the water management program agency's implementing regulations.

This requires installation commanders, when legally permissible and absent exigent circumstances, to consider the enforceable policies of water programs as requirements to be adhered to for all existing and proposed water use activities in addition to all other applicable statutory, regulatory, and policy requirements.

Installation commanders will provide applicable water program agency officials with a consistency determination, in writing, at the earliest practicable time in the planning or reassessment of the proposed installation water use activity.¹⁴⁶ This consistency determination notification must be based upon an evaluation of the relevant enforceable policies of the applicable water program. Installation water use activity consistency determinations are reserved to the sole discretionary authority of the installation commander and, as such, are not subject to state or local water management approval or judicial review.

¹⁴⁵ 16 U.S.C. § 1456 (2015).

¹⁴⁶ While specific consistency determination content requirements are detailed in the proposed policy, they may be submitted in any form or manner the installation commander chooses so long as the substantive requirements of this policy are satisfied.

The installation commander's consistency notification will state his or her determination that the proposed installation water use activity is either fully consistent or consistent to the maximum extent practicable with the applicable enforceable policies of the state or local water program. If an installation commander asserts that full consistency with applicable water program enforceable policies is prohibited, it shall clearly describe to the applicable water program agency officials the statutory provisions, legislative history, other legal authority, or operational requirements limiting or prohibiting the installation's discretion to be fully consistent with the relevant enforceable policies.

When DoD legal, regulatory, policy, or other standards applicable to a proposed installation water activity are more restrictive than standards or requirements contained in water program's enforceable policies, installations shall continue to apply the stricter federal standards. In such cases, installation commanders shall inform applicable water program agency officials in its consistency determination of the statutory, regulatory, policy, or other basis for the application of stricter federal standards.

The water program agency official may request additional information or clarification of the installation's rationale for not fully complying with its water program requirements, conditionally concur with the consistency determination, fully or partially object to the consistency determination, or provide no response at all. The proposed policy presumes water program agency concurrence if a response is not received within 60 days from receipt of the installation commander's consistency determination notification. Installation commanders should exercise good faith in responding to valid state or local water program agency requests for additional information or clarification of rationale, as well as legal and policy justifications, for the consistency determination process.

In situations where state or local water allocation management agencies respond with a consistency determination conditional concurrence, installations should attempt to modify the proposed water use activity pursuant to the water program agency's stated conditions. If the proposed conditions are not acceptable and requirements for full consistency concurrence cannot be met, installation commanders shall immediately notify the water program agency, in writing, of their rationale and justification for this determination. In these circumstances, the installation commander may treat the water allocation management agency's conditional concurrence as an objection.

In the event the water program agency either does not fully concur with, or fully or partially objects to, an installation commander's consistency determination, the installation commander and water program agency officials

should attempt to resolve their differences. If resolution has not been reached at the end of a 60-day period commencing on receipt of the water program agency's objection, installations shall not proceed with the proposed water use activity over a state agency's objection unless: (1) the installation commander has concluded that under this policy's "consistent to the maximum extent practicable" standard consistency with the enforceable policies of the water program is prohibited by existing federal law or DoD policy; (2) full consistency is incompatible with either the installation's defense mission requirements or the needs of national security, and the installation commander has clearly described, in writing, the legal and/or practicable impediments to full consistency; or (3) the installation commander has concluded that its proposed water use activity is fully consistent with the enforceable policies of the water program despite water program agency objection to, or non-concurrence with, the installation's consistency determination.

The proposed policy dispute resolution process requires installation commanders to make reasonable efforts to informally resolve disputes at the lowest supervisory level possible with applicable water program agency officials. If a resolution cannot be achieved informally, the policy implements a series of dispute resolution procedures that include elevating the dispute up the installation commander's chain of command in coordination with the applicable DoD Regional Environmental Coordinator, and, ultimately, proceeding with the installation's proposed water use activity over water program agency objection.

The proposed policy addresses handling *de minimis*, classified, and sensitive installation use activities, force majeure events, McCarran Amendment applicability, and required supporting data and records. It also provides guidance and direction to installation commanders responding to state and local water program purported permit, registration, inspection, and fees and costs requirements, as well as fines, penalties, and other attempted program enforcement actions.

The proposed policy concludes with a discussion of installation water conservation policies and practices. It notes that in response to water shortage or drought emergencies, state and local water program agencies or other executive authorities (e.g., Governor) may declare and implement emergency water conservation and drought policies, restrictions, or other similar water conservation requirements. Preserving federal sovereignty, the policy reminds DoD installation commanders that their installation water use activities are normally not subject to state or local conservation or drought program requirements. As with other water program requirements, the DoD may, as a matter of comity, voluntarily agree to cooperate with state and local officials to

the maximum extent permitted under federal law without improperly waiving federal sovereignty. Accordingly, the proposed policy attempts to do just that.

The proposed policy states that where installation compliance with state or local water laws or regulations is prohibited by federal law and/or inconsistent with the needs of national defense, installation water use activities shall, as a matter of comity, be consistent to the maximum extent practicable with water program emergency water conservation and drought policies, restrictions, orders, or other requirements in accordance with the procedures set forth below. At a minimum, installation commanders should do their part in conserving drought impacted water resources by refraining from non-mission essential water use. Examples include, but are not limited to, restrictions on watering lawns, athletic fields, golf courses, and outdoor plants; washing vehicles and paved surfaces; and filling swimming pools.

Finally, in determining installation consistency with applicable water program emergency water conservation and drought policies, restrictions, orders, or other requirements, installation commanders are directed to consider installation water conservations plans, potential adverse mission impacts, economic practicability, and other specific issues preventing program implementation.

The proposed policy directive preserves the appropriate balance between preserving DoD federal sovereignty from state and local regulatory requirements while protecting legitimate state and local rights and interests in the allocation of water resources.

III. Conclusion

Water is now generally recognized as a vital, but increasingly scarce, natural resource. Access to, and use of, self-supplied groundwater withdrawals and surface water diversions is becoming increasingly limited throughout the western states and ever-increasingly in parts of the eastern United States. Like other federal landowners, DoD installations increasingly rely on self-supplied groundwater withdrawals and surface water diversions to either fully meet or supplement contractually supplied water to accomplish their congressionally-mandated defense missions.

Balanced against these federal agency requirements is the congressionally, and judicially-recognized rights of states to choose their own system of water law and with it the ancillary right to oversee, manage, conserve, and equitably distribute water resources within their jurisdictions, including those on public lands. These rights often manifest themselves as state statutory

and local water management programs regulatory permitting and registration requirements, extraction and use fees and taxes, defined allocation quantities, use prohibitions or restrictions, mandatory conservation measures, and state administrative and judicial allocation resolution processes.

These state and local water management program requirements present several practical difficulties and legal concerns. First, the state and local water acquisition, allocation, and use requirements sometimes conflict with the installation's federal purposes. An extreme example of this conflict would be a denial of the DoD's ability to withdraw groundwater from an installation well, with the lack of such water adversely impacting national defense-related mission readiness or activity such as supplying housing area drinking water or providing water for required industrial requirements. Second, despite Congress's articulated recognition of, and deference to, state sovereignty over water allocation within state boundaries, it has not taken the steps to affirmatively waive federal sovereignty, thereby directing and authorizing full federal agency compliance with state and local water allocation regimes. This leaves DoD installations in the unique position of being a state water appropriator but outside the umbrella of state and local water management program requirements, control, and enforcement. Finally, immunity from state water allocation requirements removes the discretionary authority for installation compliance with all or any of the otherwise applicable state or local requirements. For example, the payment of state or local permit or extraction fees and submission to state administrative or judicial allocation or dispute resolution proceedings are prohibited under federal law. To the extent these restrictions give rise to local, regional, or national political or judicial conflicts, they either impede or have the potential to impede DoD installations from meeting their defense mission requirements, the resolution of which becomes a national security concern.

Unfortunately, it is not merely a simple matter of federal agencies complying with the same state and local water appropriation procedural requirements that apply to other appropriators. As discussed above, federal agencies may only comply with these requirements as permitted by federal law. Absent a valid, unequivocal congressional waiver of federal sovereign supremacy and immunity, state and local water administration laws and regulations cannot operate to limit, condition, or divest DoD installation water uses for any needs, primary or otherwise. To date, Congress has not so directed.

As demonstrated above, the DoD's voluntary implementation of a CZMA-like Federal Consistency requirement for self-service water appropriations, acquisitions, and uses would more than adequately meet the above three criteria of an effective and successful compromise policy:

uniformity, protection of federal sovereignty, and deference to legitimate state and local water resource management interests. It does so by requiring, as a matter of policy, DoD installation commanders' cooperation, coordination, and good faith efforts to ensure their federal water use activities are consistent to the maximum extent practicable, under federal law and the needs of national defense, with the enforceable policies of applicable water program general and emergency requirements.

Appendix

Department of Defense Federal Water Use Activities

1. Scope

1.1 General. This policy identifies requirements, establishes policy, and assigns responsibilities for the use, protection, documentation, and assertion of water use activity rights at Department of Defense (hereinafter "DoD") installations in the United States and its territories and commonwealths (hereinafter "DoD installations").

1.2 Applicability. This policy herein applies to DoD installation water use activities. It does not apply to water supplied to DoD installations or tenants from sources off the DoD installation pursuant to contracts with municipalities or other water suppliers.

2. Terms and Definitions

2.1 Adjudication. A judicial determination of the amount and priority of water rights in a given drainage basin. This is a special type of lawsuit to which all users of water in the basin are parties. The result of an adjudication is a decree fixing the amount and relative priorities of water rights and other essential information, such as point of diversion, beneficial use, place of use, and any limitations on the exercise of the right decreed. Typically, adjudication is a determination of rights already in existence, which may be evidenced by permit, certificate, or other facts establishing the existence of a water right.

2.2 Appropriation. A diversion of a specific amount of water and application thereof to a beneficial use.

2.3 Classified or Sensitive. The term "classified" means to protect from disclosure information pertaining to national security, national defense, or foreign policy, if the information has been properly classified in accordance with the substantive and procedural requirements of an executive order. The term "sensitive" means to protect from disclosure operational information concerning personnel, facility, and property protection, Homeland Defense, and other Anti-Terrorism/Force Protection (AT/FP)-related information.

2.4 Consistent to the Maximum Extent Practicable. The term "consistent to the maximum extent practicable" means fully consistent with the enforceable policies of applicable water allocation management programs unless:

- a. Full consistency is prohibited by existing law applicable to the DoD; or
- b. Deviation is justified because of an emergency or other similar unforeseen, exigent circumstance (e.g., situations requiring immediate action); or
- c. Full consistency is inconsistent or incompatible with DoD installation mission requirements or the needs of national defense.

2.5 *De minimis* activities. The term "*de minimis*" means those DoD installation water use activities determined to have insignificant direct or indirect (cumulative and secondary) water use effects and which the water allocation management program agency concurs are *de minimis*. *De minimis* activities shall only be excluded from water allocation management program agency review if both the DoD installation and the water allocation management program agency agree to the exclusion.

2.6 Diversion. A taking of water from its natural course or from an aquifer for conveyance to a place of use. A diversion is usually affected by a structure such as a weir, dam, guide wall, well, or the like.

2.7 Enforceable Policy. The term "enforceable policy" means water allocation management program policies that are legally binding through constitutional provisions, laws, regulations, land use plans, ordinances, or judicial or administrative decisions, by which a water allocation management program exerts control over private and public self-supplied water allocations, acquisitions, and uses and which are expressly incorporated in the applicable water allocation management program. In most circumstances, these policies will be found in the applicable water management program's authorizing statute and the water management program's implementing regulations. These enforceable policies should contain standards of sufficient specificity to guide public and private water uses. Enforceable policies need not establish detailed criteria such that a proponent of an activity could determine the consistency of an activity without interaction with the state agency. State and local water allocation management program agencies may identify management measures that are based on enforceable policies, and, if implemented, would allow the activity to be conducted consistent with the enforceable policies of the program.

2.8 Self-Supplied Water. DoD installation groundwater withdrawals and surface water diversions from water in streams, lakes, springs, reservoirs, aquifers, or other bodies of surface or groundwater on, under, touching, or otherwise appurtenant to all land owned by the United States and administered or controlled by DoD, including newly acquired, reserved, purchased, or

condemned land. It does not include water supplied to DoD installations, activities, or tenants from sources off the DoD installation pursuant to contracts or leases with municipalities or other water suppliers.

2.9 Water Allocation Management Program. Those laws and regulations adopted by a state, tribe, territory, commonwealth, or political sub-division thereof for the allocation, management, or conservation of water. It includes local and regional water authorities.

2.10 Water Allocation Management Program Agency. Any state, tribal, territorial, commonwealth, or political sub-division thereof agency or similar governmental entity responsible for water allocations, appropriations, acquisitions, water rights, water rights adjudications, and use prohibitions or restrictions.

2.11 Water Right. A water right is the right to use water. For purposes of this policy, a water right includes any use of water on the DoD installation no matter whether the use is permitted, decreed, or otherwise documented or officially recognized by state, federal, or other authority.

2.12 Water Use Activity. The term “water use activity” means any self-supplied water appropriation, acquisition, and use, including, but not limited to, ground water withdrawals and surface water diversions, performed by or on behalf of a DoD installation. This includes a wide range of DoD installation practices related to, and reasonably likely to affect, water withdrawal or use (e.g., digging wells). The term does not include rule making, grants, leasing, water purchases, or the transfer of title.

3. Policy

3.1 The DoD shall assert, maintain, and protect all DoD installation water use activities on federal lands, however acquired, where present and reasonably foreseeable water needs are necessary for accomplishment of the installation's national defense mission or missions.

3.2 In those circumstances where DoD compliance with water allocation management program requirements are not authorized under federal law, DoD installation water use activities, as a matter of comity, shall be consistent to the maximum extent practicable with the enforceable policies of the applicable water allocation management program.

3.3 DoD installation Commanders will immediately notify the Regional Commander and DoD Regional Environmental Coordinator if any water allocation management program official:

- a. Objects to a DoD installation's assertion or exercise of the installations water use activities, a refusal to comply with registration or permitting requirements, or a refusal to pay assessed fees or taxes;
- b. Issues, or attempts to issue, a permit, registration, or other administrative order purporting to regulate, condition, or limit the DoD installation's water use activities; or,
- c. Notifies the DoD installation of its intent to seek criminal, administrative, or civil enforcement of its enforceable policies arising from the DoD installation's exercise of its water use activities.

3.4 DoD installation water use activity consistency determinations are reserved to the sole discretionary authority of the installation Commander and, as such, are not subject to state or local water management approval or judicial review.

4. Federal Consistency Process

4.1 Objective. These provisions are intended to assure that all DoD installation water use activities will be undertaken in accordance with federal law and agency authorities, as well as in a manner consistent to the maximum extent practicable with applicable water allocation management program enforceable policies.

4.2 Identifying DoD installation Water Use Activities

- a. DoD installations shall review their existing and reasonably foreseeable water use activities to facilitate consistency determinations, indicating whether such water use activities are, or will be, undertaken in a manner consistent to the maximum extent practicable with the enforceable policies of applicable water allocation management program requirements.
- b. DoD installations should consult with water allocation management program agency officials at an early stage in the development of proposed water use activities to assist the DoD installation in assessing whether such activities will be consistent to the maximum extent practicable with the enforceable policies of the applicable water allocation management program.

- c. DoD installations are encouraged to coordinate and consult with water allocation management program agency officials in order to avoid waste, duplication of effort, and to reduce federal and state or local administrative burdens.

4.3 Federal Consistency Requirements

- a. Whenever legally permissible, DoD installations shall consider the enforceable policies of water allocation management programs as requirements to be adhered to in addition to existing DoD installation statutory and regulatory mandates.
- b. **Exigent Circumstances.** DoD installations shall carry out their water use activities in a manner that is consistent to the maximum extent practicable with the enforceable policies of water allocation management program to the extent exigent circumstances (e.g., situations requiring immediate action) allow. DoD installations shall confer with water allocation management program agency officials to the extent that exigent circumstances allow and shall attempt to seek their concurrence prior to addressing the exigent circumstance or circumstances. Any deviation shall be the minimum necessary to adequately address the exigent circumstances or circumstances. Once the exigent circumstance has passed, and if the DoD installation continues to carrying out a water use activity contrary to applicable water allocation management program requirements, the DoD installation shall comply with all applicable provisions of this policy to ensure that the water use activity is consistent to the maximum extent practicable with the enforceable policies of the applicable water allocation management program. Once the DoD installation addresses the exigent circumstance or circumstances or completes its emergency response activities, it shall provide the applicable water allocation management program agency officials with a description, in writing, of the nature of the exigent circumstance or circumstances, its response action or actions, and its assessment of potential or actual adverse water use effects.
- c. If a DoD installation asserts that full consistency with applicable water allocation management program enforceable policies is prohibited, it shall clearly describe, in writing, to the applicable water allocation management program agency officials the statutory provisions, legislative history, other legal authority, or

operational requirements limiting or prohibiting the DoD installations' ability to, in the exercise of its discretion, be fully consistent with the relevant enforceable policies.

4.4 Timing of Federal Consistency Determinations. DoD installations shall provide applicable water allocation management program agency officials with a consistency determination, in writing, at the earliest practicable time in the planning or reassessment of the proposed DoD installation water use activity. Consistency determinations should be prepared following development of sufficient information to reasonably determine the consistency of the water use activity with the applicable enforceable policies of the water allocation management program, but before the DoD installation reaches a significant point of decision-making in its review process (i.e., while the DoD installation has the ability to modify the proposed activity). DoD installations may, but are not required to, provide applicable water allocation management program agency officials with consistency determinations for any water use or uses prior to or existing at the effective date of this policy.

4.5 Content of a Consistency Determination

- a. The DoD installation consistency determination shall include, consistent with needs of DoD installation, activity, and national security, the following information:
 1. A detailed description of the DoD installation and its associated facilities;
 2. A brief statement that the DoD installation is exercising its federal water use activity rights;
 3. That compliance with water allocation management program laws or regulations are prohibited by federal law;
 4. That the federal consistency determination notification is made as a matter of comity and is not to be construed as a waiver of federal sovereignty;
 5. A description of the DoD installation's water use activities;
 6. The specific water allocation management program enforceable policy or policies;

7. A statement that the DoD installation's water use activity is consistent to the maximum extent practicable with the enforceable policies of the applicable water allocation management program;
 8. Land status of the DoD installation;
 9. Comprehensive data and information sufficient to support the DoD installation's consistency determination;
 10. All information on water use activity that would normally be required of an applicant for a water right from the water allocation management program agency, state, territorial, commonwealth, or political sub-division water allocation law or regulation;
 11. Any additional information requested by water allocation management program agency officials the DoD installation Commander determines is relevant, reasonable, and releasable; and
 12. A copy of this policy.
- b. The DoD installation consistency determination must be based upon an evaluation of the relevant enforceable policies of the applicable water allocation management program. A description of this evaluation shall be included in the consistency determination, or provided to the water allocation management program simultaneously with the consistency determination if the evaluation is contained in another document. Where a DoD installation is aware, prior to its submission of its consistency determination, that its water use activity is not fully consistent with the enforceable policies of the applicable state water allocation management program, the DoD installation Commander, or his/her designee, shall describe in its consistency determination the legal authority that prohibits full consistency. Where the DoD installation is not aware of any potential inconsistency until after submission of its consistency determination, the DoD installation shall submit its description of the legal authority that prohibits full consistency to the water allocation management program agency as soon as practicable.
 - c. The amount of detail in the DoD installation's consistency evaluation of applicable water allocation management program enforceable policies, water use activity descriptions, and supporting information shall be commensurate with the expected potential adverse effects of the DoD installation's proposed water use activity or activities.

- d. DoD installations may submit the necessary consistency determination and supporting information in any manner they choose so long as the substantive requirements of this policy are satisfied.
- e. When DoD statutory, regulatory, policy, judicial, or other standards are more restrictive than standards or requirements contained in the enforceable policies of applicable water allocation management programs, DoD installations shall continue to apply their stricter standards. In such cases, DoD installations shall inform applicable water allocation management program agency officials in its consistency determination of the statutory, regulatory, policy, or other basis for the application of stricter Federal standards.

4.6 Water Allocation Management Program Response

- a. Water allocation management program officials should inform the DoD installation of their concurrence with, or objection to, the DoD installation's consistency determination.
- b. DoD installation Commanders may presume water allocation management program agency concurrence if a water allocation management program agency response is not received within 60 days from receipt of the DoD's consistency determination and supporting information.
- c. Water allocation management program agency concurrence shall not be presumed in cases where water allocation management program agency officials request, in writing, within the 60-day period, an extension of time to review the matter. DoD installation Commanders shall normally approve one properly submitted water allocation management program agency request for an extension period of 30 days or less. In considering whether a longer or additional extension period is appropriate, DoD installation Commanders should consider the magnitude and complexity of the proposed water use activity, its potential for significant adverse impacts on the applicable water allocation management program, the complexity of the federal consistency analysis, and the amount of information contained in the consistency determination.
- d. Final DoD installation federal water use activities shall not be taken sooner than 60 days from the applicable water allocation management program agency's receipt of the DoD installation's consistency

determination notification, unless water allocation management program agency officials concur, their concurrence is presumed per sub-section (b) above, or both the DoD installation and water allocation management program agency officials mutually agree, in writing, to an alternative agreement.

- e. Time limits on concurrence. Normally, a water allocation management program agency cannot place an expiration date on its concurrence. If a water allocation management program agency believes that an expiration date is necessary, the water allocation management program agency and the DoD installation Commander may agree, in writing, to a mutually agreeable and reasonable time limit. If there is no agreement, later phases of, or modifications to, the DoD installation's water use activity not evaluated at the time of the original consistency determination will require either a separate or supplemental consistency determination.

4.7 Water allocation management program objection

- a. Water allocation management program agency officials may object to a DoD installation's consistency determination. If not submitted in the water allocation management program agency's response to a DoD installation's consistency determination, DoD installation Commander shall request, in writing, the water allocation management program agency's reasons for its objection and supporting information. Specifically, the water allocation management program agency objection should describe:
 1. The specific applicable enforceable policies (including citations) of the water allocation management program water appropriation management program;
 2. How the proposed federal water use activity may be inconsistent with their applicable enforceable policies;
 3. Alternative measures (if they exist) that, if adopted by the DoD installation, would allow the federal water use activity to proceed in a manner consistent to the maximum extent practicable with the enforceable policies of the water allocation management program. Failure to describe alternatives does not affect the validity of the water allocation management program agency's objection.

- b. If the water allocation management program agency's objection is based upon a finding that the DoD installation has failed to supply sufficient information, the water allocation management program agency's response must describe the nature of the information requested and the necessity of having such information to determine the consistency of the DoD installation's water use activity with the applicable enforceable policies of the water allocation management program.
- c. In the event the water allocation management program agency objects to the DoD installation's consistency determination, the DoD installation Commander and water allocation management program agency officials should attempt to resolve their differences. If resolution has not been reached at the end of a 60-day period commencing on receipt of the water allocation management program agency's objection, DoD installations shall not proceed with the proposed water use activity over a water allocation management program agency's objection unless:
 1. The DoD installation Commander has concluded that under this policy's "consistent to the maximum extent practicable" standard, consistency with the enforceable policies of the water allocation management program is prohibited by existing federal law or DoD policy;
 2. Full consistency is incompatible with either the DoD installation's defense mission requirements or the needs of national security, and the DoD installation Commander has clearly described, in writing, the legal and/or practicable impediments to full consistency; or
 3. The DoD installation Commander has concluded that its proposed water use activity is fully consistent with the enforceable policies of the water allocation management program despite the water allocation management program agency's objection to, or non-concurrence with, the DoD installation's consistency determination.
- d. If a DoD installation decides to proceed with a proposed water use activity that is objected to by a water allocation management program agency, or to follow an alternative suggested by the water allocation management program agency, the DoD installation shall notify water allocation management program agency officials of its decision, in writing, prior to proceeding with the proposed water use activity.

- e. Prior coordination with, and approval of, the cognizant Regional Commander and DoD Regional Environmental Coordinator is required before a DoD installation proceeds with a proposed water use activity objected to by a water allocation management program agency.

4.8 Conditional Concurrence

- a. DoD installations should cooperate with water allocation management program agency officials to develop conditions that, if agreed to during the water allocation management program agency's federal consistency review period and included in a DoD installation's final consistency determination, would allow the water allocation management program agency to concur with the DoD installation's proposed water use activity. If instead, a water allocation management program agency issues a conditional concurrence, water allocation management program agency officials should include in their response the exact conditions which must be satisfied, an identification of the relevant specific enforceable policies, and an explanation of why the conditions are necessary to ensure full consistency with specific enforceable policies of the state water allocation management program.
- b. DoD installations shall immediately notify the water allocation management program agency, in writing, if the proposed conditions are not acceptable and provide a rationale for this determination.
- c. DoD installations should attempt to modify the proposed water use pursuant to the water allocation management program agency's stated conditions.
- d. If the requirements of a conditional concurrence cannot be met, the DoD installation Commander should treat the water allocation management program agency's conditional concurrence notification as an objection.

4.9 Supplemental Coordination for Proposed Water Use Activities

For proposed DoD installation water use activities that were previously determined by the DoD installation Commander to be consistent with the enforceable policies of the water allocation management program, but which have not yet begun, DoD installations shall further coordinate with the water allocation management program agency officials and prepare a supplemental federal consistency determination if the DoD installation's proposed water use

activity is substantially different than originally described. Substantially different water use activities are reasonably foreseeable if:

- a. The DoD installation makes substantial changes in the proposed federal water use activity that are relevant to state water allocation management program enforceable policies;
- b. There are significant new circumstances (i.e., significant changes in military mission, water use need, proposed water use activity, or relevant enforceable policies); or
- c. There is significant new information, relevant to the proposed water use activity and the proposed activity's effect on state water uses or resources.

4.10 Permit Requirements

- a. Water allocation management program agencies shall not require DoD installations to obtain water allocation management program permits to process the DoD installation's federal consistency determinations unless such permitting is otherwise required or authorized by federal law and allowed by the Comptroller General of the United States.
- b. In no case may a water allocation management program agency stay the consistency review period or base an objection on the failure of a DoD installation's to obtain a permit inconsistent with this policy.
- c. Prior coordination with, and approval of, the DoD installation's cognizant Regional Commander and DoD Regional Environmental Coordinator is required before DoD installation compliance with any water allocation management program agency permitting requirements.

4.11 Water Allocation Management Program Fees

- a. Water allocation management program agencies shall not assess DoD installations with a fee to process the DoD installation's consistency determination unless payment of such fees is required by other federal law and allowed by the Comptroller General of the United States.
- b. In no case may a water allocation management program agency stay its consistency review or base an objection on the failure of a DoD installation to pay an assessment not otherwise required or authorized

by federal law and allowed by the Comptroller General of the United States.

- c. Prior coordination with, and approval of, the DoD installation's cognizant Regional Commander and DoD Regional Environmental Coordinator is required before DoD installation payment of any water allocation management program agency program-assessed fees.

4.12 *De Minimis* Activities. DoD installation Commanders are encouraged to review their existing and reasonably foreseeable water use activities to identify *de minimis* activities and request water allocation management program agency concurrence that these *de minimis* activities should not be subject to further DoD installation consistency determinations and water allocation management program agency concurrence reviews. If the water allocation management program agency objects to the DoD installation's *de minimis* determination, the DoD installation Commander must provide the water allocation management program agency with a water use activity consistency determination.

4.13 Classified or Sensitive Activities. Classified or sensitive federal water use activities are exempt from the requirements of this policy. Under the "consistent to the maximum extent practicable" standard, DoD installation Commanders shall provide to the water allocation management program agency a description of the proposed water use activity that it is legally permitted to release, or that does not otherwise breach, the classified or sensitive nature of the activity. In those situations when DoD installations cannot disclose the specifics of its federal water use activities to water allocation management program agency officials, the DoD installation Commander shall, if practicable, proceed with water use activity in a manner consistent to the maximum extent practicable with the enforceable policies of the water allocation management program and not seek water allocation management program review and concurrence.

4.14 Dispute Resolution

- a. If a dispute arises under this policy, DoD installation Commanders should make reasonable efforts to informally resolve disputes at the lowest supervisory level possible with applicable water allocation management program agency officials. The disputing party shall engage the other party or parties in informal dispute resolution among relevant DoD installation and water allocation management program agency officials. During this informal dispute resolution period, the parties shall meet and/or confer as many times as are necessary to discuss and attempt resolution of the dispute.

- b. If resolution cannot be achieved informally, the following dispute resolution procedures shall be implemented:
 1. Within 30 days after: (1) DoD installation Commander's decision to proceed with the proposed water use activity over water allocation management program agency objection; or (2) any action that leads to, or generates, a dispute, the disputing party shall submit to the other party a written statement of dispute setting forth the nature of the dispute, the water use activity affected by the dispute, the disputing party's position with respect to the dispute, and the information the disputing party is relying upon to support its position.
 2. Disputes for which agreement cannot be reached through informal dispute resolution shall be referred by the DoD installation to the cognizant Regional Commander for resolution in coordination with the DoD Regional Environmental Coordinator.
 3. The pendency of any dispute under this paragraph shall not affect the DoD installation's execution of the proposed water use activity. DoD installation Commanders are, however, encouraged to postpone action pending dispute resolution.
 4. Prior coordination with, and approval of, the cognizant Regional Commander, after conferring with the DoD Regional Environmental Coordinator, is required before initiating the dispute resolution process or proceeding with any disputed proposed water use activity.
 5. Within 21 days of resolution of a dispute pursuant to the procedures specified in this sub-paragraph, the DoD installation Commander shall incorporate the resolution and final determination into the DoD installation's consistency determination and implement the final determination as required.

4.15 Force Majeure

- a. A Force Majeure, for the purpose of this policy, shall mean any event arising from causes beyond the control of the DoD installation that causes a delay in or prevents the performance of any obligation under this policy, including but not limited to:
 1. Acts of God;

2. Fire;
 3. War;
 4. Insurrection;
 5. Civil disturbance;
 6. Explosion;
 7. Unanticipated breakage or accident to machinery, equipment, or lines of pipe despite reasonably diligent maintenance;
 8. Adverse weather conditions that could not be reasonably anticipated;
 9. Unusual delay in transportation due to circumstances beyond the control of the DoD;
 10. Restraint by court order or order of competent public authority;
 11. Inability to obtain, at reasonable cost and after exercise of reasonable diligence, any necessary authorizations, approvals, permits, or licenses due to action or inaction of any governmental agency or authority other than the DoD;
 12. Delays caused by compliance with applicable statutes or regulations governing contracting, procurement, or acquisition procedures, despite the exercise of reasonable diligence; and
 13. Insufficient availability of appropriated funds, if the DoD installation or responsible Budget Submitting Office made a timely request for such funds as a part of the budgetary process.
- b. A Force Majeure shall also include any strike or other labor dispute, whether or not within control of the DoD installation affected thereby. Force Majeure shall not include increased costs or expenses of response actions, whether or not anticipated at the time such response actions were initiated.
 - c. When circumstances which may delay or prevent the completion of the DoD's obligation under this policy are caused by a Force Majeure

event, the DoD installation shall notify applicable water allocation management program agency officials, by verbal report, within 48 hours after the DoD installation first became aware of these circumstances. Within 15 days of the verbal notification, the DoD installation shall provide water allocation management program agency officials, in writing, a description of the Force Majeure event and an explanation of adverse effects on DoD installation's ability to ensure their water use activities are consistent to the maximum extent practicable with applicable water allocation management program enforceable policies. The DoD installation Commander shall exercise best reasonable efforts to avoid or minimize adverse impacts.

5. Water Rights Adjudications: The McCarran Amendment

- a. The McCarran Amendment, 43 U.S.C. § 666, grants Congressional consent to the joinder of the United States as a defendant in comprehensive water rights adjudications. Comprehensive water rights adjudication is a state lawsuit or administrative action to adjudicate the water rights of all of the claimants to a particular watercourse. The McCarran Amendment's waiver of federal supremacy does not extend to private suits against the United States, operate to limit federal water rights, or require federal agencies to comply with state or local registration, permitting, or fee requirements (designed to assign future water rights).
- b. Once the United States is properly joined in a comprehensive adjudication action, there is limited time to perfect and submit claims for water rights. The U.S. Department of Justice has the sole authority to appear and represent the interests of the United States in these actions. To ensure proper representation and to avoid the potential loss or diminution of federal water rights, DoD installation Commanders shall, after consultation with their respective Staff Judge Advocate or General Counsel, immediately notify the Regional Commander and DoD Regional Environmental Coordinator of any state legal or administrative actions involving the potential adjudication of DoD installation water use activities or water rights.

6. Permit/Registration Requirements. Water allocation management programs typically require persons or entities acquiring self-supplied water, including federal agencies, to obtain a permit or register their activities. Generally, water permitting or registration requirements are not prerequisites to DoD installation water use activities.

6.1 General. DoD installations will ordinarily not register or apply for permits for water use activities unless required by federal law and allowed by the Comptroller General of the United States.

6.2 General Guidance. To the extent DoD installation Commanders submit, as a matter of comity, information in response to water allocation management program requirements, DoD installation Commanders shall include the following general disclaimer in all permits and cover letters to state officials:

"The [water appropriation][water use][well][surface diversion] in question is intended to supply water deemed necessary by the [DoD installation] [activity] Commander to meet its statutory defense mission(s). This information is provided as a matter of comity and is not to be construed as a waiver or modification of the sovereign immunity of the United States, the Department of Defense, or [service]."

7. Inspections. The DoD has federal sovereign rights within the exclusive federal enclave of its DoD installations and is not required to allow water allocation management program agency officials to conduct inspections of DoD installation water use activities, facilities, or locations. That said, DoD installation Commanders are encouraged, as a matter of comity, to invite and allow applicable water allocation management program agency officials to visit, perform informational fact-finding, and conduct assessments of DoD installation water use activities, facilities, and locations deemed by the DoD installation Commander to be in legitimate furtherance of valid water allocation management program interests.

8. Fines and Penalties. Absent a valid Congressional statutory waiver of federal sovereignty, DoD installations shall not pay water allocation management program agency-assessed fines or penalties arising from any DoD installation water use activities.

9. Water Allocation Management Program Fees

9.1 General. In addition to registration and permitting requirements, water allocation management program agencies may attempt to require DoD installations to pay registration and/or permitting processing fees as well as extraction/diversion charges (typically fixed at a uniform rate per acre-foot) for groundwater extracted or surface water diverted on DoD installations or activities. The DoD's authority to pay registration/permit processing fees, extraction charges, or other similar assessments is significantly limited by federal law. Absent a federal statute authorizing such payment, the payment of

DoD installation water use activity fees may violate the federal Anti-Deficiency Act, 31 U.S.C. § 1341(a).

9.2 DoD policy is that water allocation management program processing fees and/or extraction charges related to DoD installation water use activities will ordinarily be presumed to be impermissible taxes for which federal sovereignty has not been Congressionally waived and, therefore, cannot constitutionally be imposed upon the federal government.

9.3 DoD installations may pay water allocation management program fees, extraction charges, or other similar assessments only if the payment is:

- a. Authorized or required by federal law;
- b. Agreed to by the Comptroller General of the United States; and
- c. Compensation on a *quantum meruit* basis for the fair and reasonable value of services actually rendered to the DoD installation.

9.4 DoD installation Commanders shall not pay any water allocation management program agency-assessed processing fees, extraction charges, or other similar assessments related to DoD installation water use activities without the following:

- a. Consultation with his or her Staff Judge Advocate or General Counsel;
- b. Coordination with the DoD Regional Environmental Coordinator; and
- c. Prior approval by the Regional Commander.

10. No Waiver of Rights. In its correspondence or dealing with water allocation management program agencies, DoD installations shall seek acknowledgement that the United States does not waive or otherwise forfeit any federal right or interest.

11. Costs. DoD installations shall include the cost of being either fully consistent, or consistent to the maximum extent practicable with the enforceable policies of state, territorial, commonwealth, or political sub-divisions thereof water allocation management programs, in their budget and planning processes, to the same extent that the activity would plan for the cost of complying with other facility or operational requirements. In cases where the cost of being consistent to the maximum extent practicable with the enforceable policies of water allocation management programs was not included in the DoD

installation's budget and planning processes, the DoD installation Commander should determine the amount of funds needed and seek additional funds from appropriate Service authorities.

12. Supporting Data and Records

12.1 Water Rights Coordinators/Points of Contact. DoD installation Commanders shall designate, in writing, a Water Rights Coordinator to supervise implementation of this policy.

12.2 Identification of Water Rights and Supporting Data and Records. Failures to adequately document, assert, and preserve self-supplied federal water rights may result in the loss of federal water use activity rights.

12.2.1 Water Use Activity Audits. DoD installation Commanders shall conduct annual audits of all water use activities and maintain the following information:

- a. Name of withdrawal or diversion structure (e.g., well number, reservoir);
- b. Location of point of diversion (legal description);
- c. Means of diversion (e.g., dam, well, weir);
- d. Source (name of stream or aquifer);
- e. Depth of well(s);
- f. Amount of diversion (for direct flow surface diversion, such as ditches and pipelines, the maximum diversion rate in cubic feet per second; for wells, the diversion rate in cubic feet per second or gallons per minute; for reservoirs, the active storage capacity in acre feet);
- g. Date work on appropriation was initiated;
- h. Date water was applied to DoD installation mission use;
- i. Date the DoD installation was reserved from the public domain or the date the land was acquired;
- j. Use(s) to which water is applied, for example, municipal, industrial, irrigation, domestic, military (including training, testing of vehicles and equipment, troop morale and welfare), fish and wildlife, recreation;

- k. Means of conveyance (e.g., ditch, pipeline, or combination);
- l. Dimensions of means of conveyance;
- m. Pump nameplate capacity (wells and pipelines);
- n. Copies of all documents regarding the acquisition and history of all water rights acquired. Such documentation includes, but is not limited to, the following:
 - 1. Court decrees, permits, or certificates;
 - 2. History of use, to include records of amounts diverted and used, times of use, and uses made of the water;
 - 3. Proof of dates of initiation of work and application of water to DoD installation's mission use (e.g., plans, built drawings, photographs, maps, completion reports, newspaper articles, or other records);
 - 4. Proof of amounts used, such as diversion records, well pump test, gauging reports, or calculations;
 - 5. Any other documents pertaining to the water use activity;
 - 6. Any other information the DoD installation Commander, Regional Commander, or DoD Regional Environmental Coordinator deems useful or necessary or that the particular state or local authority maintains or considers necessary.

13. Water Conservation

13.1 General. Since access to adequate water supplies is necessary for future DoD installation readiness and sustainability, it is DoD policy to conserve water resources and implement water conservation programs.

13.2 DoD installations shall:

- a. Develop and implement a plan to for DoD installation water uses;
- b. Review all DoD installation water uses;
- c. Conduct a water use prioritization survey;

- d. Establish DoD installation water conservation goals;
- e. Implement a DoD installation water conservation plan;
- f. Implement economically practicable and cost-effective water conservation measures;
- g. Ensure that all economically practicable water conservation measures are taken;
- h. Reduce DoD installation water usage by implementing life cycle cost-effective water efficiency programs and measures; and
- i. Assess and implement measures to improve the efficiency of DoD installation or activity water use and conservation programs.

14. Emergency Water Conservation and Drought Programs

14.1 General. In response to water shortage or drought emergencies, water allocation management programs and other state, tribal, territorial, commonwealth, and political sub-divisions thereof officials may declare and implement emergency water conservation and drought policies, restrictions, or other similar water conservation requirements. These measures usually include mandatory reductions in overall water consumption, rate increases, restrictions on non-essential water uses, or any combination thereof.

14.2 Policy. DoD installations are normally not subject to state, tribal, territorial, or commonwealth emergency water conservation or drought program requirements.

14.3 Federal Consistency. In those circumstances where DoD installation compliance with state or local water laws or regulations is prohibited by federal law and/or inconsistent with the needs of national defense, DoD installation water use activities shall, as a matter of comity, be consistent to the maximum extent practicable with water allocation management program emergency water conservation and drought policies, restrictions, orders, or other requirements in accordance with the procedures set forth below. At a minimum, DoD installations should do their part in conserving drought impacted water resources by refraining from non-mission essential water use. Examples include, but are not limited to, restrictions on watering lawns, athletic fields, golf courses, and outdoor plants; washing vehicles and paved surfaces; and filling swimming pools.

14.4 Mission Impact Assessment. In determining DoD installation consistency with applicable water allocation management program emergency water conservation and drought policies, restrictions, orders, or other requirements, DoD installation Commanders are directed to consider DoD installation water conservations plans, potential adverse mission impacts, economic practicability, and other specific issues preventing program implementation. If DoD installation core mission or missions will be, or are reasonably likely to be, negatively impacted, DoD installation Commanders should consult with their Regional Commander and DoD Regional Environmental Coordinator prior to declining to implement water management program agency-recommended emergency water conservation and drought measures.

“POURING NEW WINE INTO OLD BOTTLES”: UNDERSTANDING THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES WITHIN THE CYBER DOMAIN

Lieutenant Commander Christopher P. Toscano, JAGC, USN*

“Cyber attacks are not what makes the cool war 'cool.' As a strategic matter, they do not differ fundamentally from older tools of espionage and sabotage.”

— Noah Feldman¹

I. Introduction

Warfare has evolved. Advancements in technology and the advent of the internet have created new issues that current bodies of law do not directly reference or address. Traditional notions of armed attack and invasion, which were transparent over the course of the twentieth century, are now reconsidered in light of cyber domain.² Given an “inability to live at peace,” humanity has already developed and employed weapons vis-à-vis the cyber domain as illustrated through the Stuxnet incident.³ Through Stuxnet, humanity has demonstrated that computer-originated attacks can result in kinetic effects. Equally concerning, the cyber domain has created a new battlefield where traditional understandings of “combatants” require reexamination. While

* Lieutenant Commander Toscano is an active-duty Navy Judge Advocate and 2014 LLM Graduate of the George Washington University Law School. The author would like to thank Professors Paul Rosenzweig and Marc Warren for their contributions to this article. The author would also like to thank his wife, Aki, for her enduring support: 本当にありがとう愛貴ちゃん！ The positions and opinions expressed in this article are those of the author and do not represent the views of the United States Government, the Department of Defense, or the United States Navy.

¹ *Read an Excerpt of Noah Feldman's 'Cool War,'* ABC NEWS (June 27, 2013), <http://abcnews.go.com/blogs/politics/2013/06/read-an-excerpt-of-noah-feldmans-cool-war/>.

² Ellen Nakashima, *In Cyberwarfare, Rules of Engagement Still Hard to Define*, WASHINGTON POST (Mar. 10, 2013), http://articles.washingtonpost.com/2013-03-10/world/37605577_1_officials-debate-cyber-command-attack.

³ P.W. SINGER, *WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN THE 21ST CENTURY* 5 (2009); Stuxnet was a computer generated virus allegedly used to attack computer-based controllers within the Natanz nuclear enrichment plant in Iran. See Kim Zetter, *An Unprecedented Look At Stuxnet, The World's First Digital Weapon*, WIRED (Nov. 3, 2014), <http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

conventional warfare presented barriers to entry, the cyber domain has greatly enabled civilian participation in cyber hostilities. With the possibility of this trend, governments will need to develop a legal framework for responding to civilians who directly participate in cyber hostilities.

In physical warfare settings, the principle of distinction requires belligerents to differentiate between combatants and civilians under the Law of Armed Conflict (LOAC). Under LOAC, civilians enjoy protection from being the direct target of armed attack. The notion of Direct Participation in Hostilities (DPH) provides that a civilian loses this protection for undertaking combat operations against military forces in an armed conflict.⁴ This concept became relevant in the U.S. campaigns in Iraq, Afghanistan, the Global War on Terror, and other overseas contingency operations. In these conflicts, U.S. forces confronted the problem by positively identifying and engaging a civilian determined to be directly participating in hostilities. Combining the complexity of DPH with the cyber domain presents a conundrum because, unlike traditional warfare, civilians who can directly participate in cyber hostilities need not be physically located within the theater of hostilities. A hacker who undertakes hostilities can attack from any location in the world with a laptop and internet access. Therefore, the issue of direct participation in cyber hostilities (DPCH) has many factors that will require analysis in order to develop a legal framework for response.

This article stands for the proposition that a civilian who directly participates in hostilities in the cyber domain forfeits protection and becomes a lawful target. In support, this article will first highlight the background and law applicable to DPCH in general. In particular, this article will discuss the factors that render a civilian targetable by analyzing the traditional framework of DPH as applied through the Tallinn Manual.⁵ This discussion will include an understanding of what constitutes an “attack” and provide examples of which hostile roles render civilians targetable. Next, this article will discuss some of the challenges that leaders will confront in responding to issues involving DPCH. These issues include sovereignty and “targeting law” under LOAC. However, this article will provide a framework that contemplates non-kinetic, kinetic, and covert action.

⁴ Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 51(3), *adopted* June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 13(3), *adopted* June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II].

⁵ TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

II. Background: Direct Participation in Hostilities, Cyber Warfare, and the Law

Currently, there is no clear international consensus on many cyber warfare (CW) issues, least of all DPCH. Moreover, customary international law (State practice and *opinio juris*) has not developed or crystallized as found in other areas of International Humanitarian Law (IHL).⁶ The ability to detect and defend against such attacks, whether State-sponsored or not, has become exceedingly difficult given the speed and regularity of occurrences within the cyber domain generally. On the subject of “imminence” alone, U.S. Government officials struggle to develop policy that applies traditional concepts to determine whether a strike in self-defense is justified or is preventative war and thus prohibited as an unprovoked act of aggression.⁷ Furthermore, unlike traditional combat, IHL applicability to CW has not been tested before the International Court of Justice (ICJ).⁸ Therefore, CW does not cleanly fit into the hostilities paradigm for which LOAC was created.⁹ It is analogous to pouring a new wine into an old bottle.¹⁰

Nevertheless, IHL will serve as a baseline to regulate the conduct of CW until greater international consensus is reached. The fact that IHL does not specifically reference cyber operations does not imply that such operations are not subject to IHL, especially given the possibilities of physical harm caused by CW.¹¹ Thus, as an international cyber warfare legal framework does not currently exist, the applied “law” is national policy interpreting and incorporating IHL as a foundation. Given the Frankenstein-like nature of this framework and uncertainties associated with cyber weapons, many national policies will not be readily transparent.¹² For example, many of the U.S. authorities and policies applicable to CW remain classified and withheld at the

⁶ Jean-Marie Henckaerts, *Study on Customary International Humanitarian Law: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict*, 87 INT’L REV. RED CROSS 175, 190 (2005); Yoram Dinstein, Keynote Address at the 2012 Naval War College International Law Conference: Concluding Thoughts (June 27, 2012) in 89 INT’L LAW STUD. 276, 280 (2013). LOAC is also referred to as the “International Humanitarian Law” (abbreviated as “IHL”).

⁷ Nakashima, *supra* note 2.

⁸ David Turns, *Cyber Warfare and the Notion of Direct Participation in Hostilities*, 17 J. CONFLICT & SEC. L. 279, 282 (2012).

⁹ Michael Schmitt, *Classification of Cyber Warfare*, 17 J. CONFLICT & SEC. L. 245, 246 (2012).

¹⁰ Symposium, *When Is a Virus a War Crime—Targetability and Collateral Damage Under The Law of Armed Conflict*, 3 NAT’L SECURITY L. BRIEF 75, 88 (2012).

¹¹ Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INT’L REV. RED CROSS 533, 540 (2012).

¹² David Sanger & Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, N.Y. TIMES (Feb. 3, 2013), <http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html>.

highest levels.¹³ At a minimum, the United States has acknowledged IHL's applicability to CW.¹⁴ Moreover, U.S. policy runs parallel with the experts who authored the Tallinn Manual from NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE), who argue that traditional notions of IHL apply to CW.¹⁵ Therefore, this article will analyze DPCH through IHL and the Tallinn Manual as a developmental framework.

Within IHL, the principle of distinction between combatants and civilians serves as the starting point for DPCH. While principally derived from customary international law and the 1907 Hague Convention, contemporary notions of distinction are codified in Article 48 of Additional Protocol I (AP I) to the 1949 Geneva Conventions, which provides: "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."¹⁶ Thus, civilians enjoy protection from an armed attack as a generally accepted principle under IHL.¹⁷ Under the principle of distinction, parties to a conflict are required to distinguish between the civilian population and objects, and from otherwise lawful targets (e.g., military combatants).¹⁸ The United States and CCD COE acknowledged this requirement of distinction is required in CW.¹⁹

The notion of DPH, derived from Article 51(3) of AP I, provides that civilians shall enjoy protection from armed attack "unless and for such time as they take a direct part in hostilities" for international armed conflicts (IAC).²⁰ The notion is virtually identical for non-international armed conflicts (NIAC) as

¹³ *Id.*

¹⁴ Harold H. Koh, *International Law in Cyberspace*, 54 HARV. INT'L. L.J. 1, 3 (2012) ("But the United States has made clear our view that established principles of international law do apply in cyberspace."); See also Michael Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. 13, 15 (2012).

¹⁵ Schmitt, *supra* note 14, at 15. ("The relative congruency between the U.S. Government's views, as reflected in the Koh speech, and those of the International Group of Experts is striking. This confluence of a state's expression of opinio juris with a work constituting 'the teachings of the most highly qualified publicists of the various nations' significantly enhances the persuasiveness of common conclusions.")

¹⁶ Additional Protocol I, *supra* note 4, art. 48.

¹⁷ Avril McDonald, *The Challenges to International Humanitarian Law and the Principles of Distinction and Protection from the Increased Participation of Civilians in Hostilities*, ASSER INSTITUTE (Apr. 2004), http://www.asser.nl/upload/wihl-webroot/documents/cms_ihl_id70_1_McDonald%20DPH%20-%20April%202004.doc.

¹⁸ *Id.*

¹⁹ Schmitt, *supra* note 14, at 25.

²⁰ Additional Protocol I, *supra* note 4, art. 51(3).

codified within Article 13(3) of Additional Protocol II (AP II).²¹ Thus, civilians who directly participate in hostilities forfeit their protections and can be lawfully targeted. While civilians are subject to lawful targeting while taking direct part in hostilities, they are only lawful targets “for such time as” or while they actually commit hostile acts directly producing harmful effects to an enemy.²² This preceding language providing for a temporal requirement remains controversial. Institutions such as the International Committee of the Red Cross (ICRC) interpret this section very restrictively to mean that such civilians can only be targeted until he or she has returned to the pre-deployment location.²³ Thus, if a civilian conducts repeated attacks, that civilian will regain protection upon return from each engagement.²⁴ This remains highly debated among scholars and the ICRC. Other scholars take a broader view, allowing for targeting of a civilian long after he or she has lost protection.²⁵ For the purposes of cyber-conflict, the CCD COE agreed that the temporal requirement would at least include actions immediately preceding or subsequent to the qualifying act.²⁶ However, the CCD COE experts were split on the time between repeated attacks.²⁷ Thus, this issue is unresolved in both physical and cyber domains and will become a policy decision vis-à-vis rules of engagement or operational orders. This article will assume a broad view allowing for targeting in between attacks.

III. The Cumulative Factors of DPCH

While the ICRC has not published similar comprehensive guidance on DPCH or CW, the ICRC’s DPH guidance remains helpful as discussed *infra*. Moreover, the ICRC contributed to the development of the Tallinn Manual and generally agrees with the rules developed with some exceptions.²⁸ In particular, many of the notions for resolving DPCH issues are derived from the ICRC’s interpretive guidance on DPH. Thus, the Tallinn Manual remains the most comprehensive work that serves as DPCH guidance within the framework of IHL. Rule 35 of the Tallinn Manual provides that an act of direct participation in hostilities by civilians renders them liable to be attacked, by cyber or other

²¹ Additional Protocol II, *supra* note 4, art. 13(3).

²² *Id.*

²³ NILS MELZER, ICRC INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 70–71 (2009), *available at* <http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf> [hereinafter ICRC DPH GUIDANCE].

²⁴ *Id.* (discussing the so-called “revolving door” of protection).

²⁵ Bill Boothby, “*And for Such Time As*”: *The Time Dimension to Direct Participation in Hostilities*, 42 NYU J INT’L & POL 741, 743 (2010).

²⁶ TALLINN MANUAL, *supra* note 5, 120–21 (Michael N. Schmitt ed., 2013).

²⁷ *Id.*

²⁸ ICRC Resource Centre, *What Limits Does the Law of War Impose on Cyber Attacks?*, INT’L COMM. OF THE RED CROSS (Jun. 28, 2013), <http://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm>.

lawful means.²⁹ Similar to AP I and AP II, Rule 35 describes that civilians are targetable “for such time as he or she is engaged in the qualifying act of direct participation.”³⁰ Rule 35 sets forth the three cumulative criteria (threshold of harm, direct causation, and belligerent nexus) for qualification of an act as direct participation in cyber hostilities that are derived from the ICRC interpretive guidance.³¹ This rule also provides discussion regarding specific nuances within each of the three factors require case-by-case consideration in order for a civilian to be targeted for losing protection as a result of DPCH.³²

A. Understanding an Attack: Threshold of Harm

Per Article 49(1) of AP I, “attacks” are acts of violence against the adversary, whether in offense or in defense.³³ To illustrate, military convoys in Iraq or Afghanistan would be able to target, in self-defense, a roadside Improvised Explosive Device (IED) bomber or sniper for engaging in a hostile act amounting to an attack. On the other hand, a civilian who simply stands in the middle of the road holding up a sign in protest does not qualify as an attack. Targeting this protestor would be prohibited under IHL unless that civilian committed or attempt to commit an act that amounts to direct participation. By analogy, the aforementioned Stuxnet worm would clearly illustrate a kinetic attack given the resultant physical damage to Iranian centrifuges.³⁴ Conversely, the same conclusion would not easily be reached for “hacktivists,” who protest by spamming computer networks with protest e-mails.³⁵ Therefore, to understand the definition of “cyber-attack,” an analysis of the “threshold of harm” associated with it is required. Factors involved in this analysis include: “the context of the event, the actor perpetrating the action (recognizing

²⁹ TALLINN MANUAL, *supra* note 5, at 118.

³⁰ *Id.*

³¹ *Id.*

³² *Id.* at 119-121.

³³ Additional Protocol I, *supra* note 4, art. 49(1); *see also* TALLINN MANUAL, *supra* note 5, at 106. (“[I]t is the use of violence against a target that distinguishes attacks from other military operations. Non-violent operations, such as psychological cyber operations or cyber espionage, do not qualify as attacks. ‘Acts of violence’ should not be understood as limited to activities that release kinetic force. . . . In this regard, note that chemical, biological, or radiological attacks do not usually have a kinetic effect on their designated target, but it is universally agreed that they constitute attacks as a matter of law.”)

³⁴ *60 Minutes: Stuxnet: Computer Worm Opens New Era of Warfare* (CBS television broadcast Jul. 1, 2012), available at <http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-01-07-2012/>.

³⁵ Hacktivism is defined as the use of computer hacking to help advance political or social causes. *See* Mark Manion & Abby Goodrum, *Terrorism or Civil Disobedience: Toward a Hacktivist Ethic*, 30 COMPUTERS & SOC’Y 14 (2000).

challenging issues of attribution in cyberspace), the target and location, [and] effects and intent, among other possible issues.”³⁶

The Department of Defense (DoD) defines “cyber-attack” as:

A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary’s critical cyber systems, assets, or functions. The intended effects of cyber-attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or [command and control] capability. A cyber-attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber-attack may be widely separated temporally and geographically from the delivery.³⁷

The U.S. definition provides some inference that a cyber-attack need not physically destroy systems to qualify as an attack. Rather, disruption of these systems will suffice as meeting a threshold of harm.³⁸

By comparison, the ICRC’s DPH guidance provides some level of amplification on this point, despite not directly speaking about DPCH or CW specifically. The ICRC indicates that the threshold of harm for DPH is satisfied when the civilian’s actions adversely affect military operations or the military capacity of a party to the conflict.³⁹ The ICRC states that the denial of an adversary’s military use of certain objects, equipment, and territory would reach the required threshold of harm.⁴⁰ The ICRC specifically notes that the electronic interference with military computer networks would fall into this category of denial, whether accomplished through computer network attacks (CNA) or computer network exploitation (CNE).⁴¹ As cybersecurity strategist Joshua

³⁶ Koh, *supra* note 14, at 4; *see also* Schmitt, *supra* note 14, at 19.

³⁷ Memorandum from Vice Chairman of the Joint Chiefs of Staff, to Chiefs of the Military Services et al., subject: Joint Terminology for Cyberspace Operations (Nov. 2010) [hereinafter “Joint Terminology for Cyberspace Operations”].

³⁸ *Id.*

³⁹ ICRC DPH GUIDANCE, *supra* note 23, at 48.

⁴⁰ *Id.*

⁴¹ *Id.* at 48. CNA is defined as a “category of fires employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target system or computer networks, or the systems/networks themselves.”; CNE is defined as “[e]nabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data about target or adversary automated

Corman notes, a cyber-attack is essentially no different from electronic warfare where an adversary denies military use of equipment through jamming or interfering with a network.⁴² Thus, a civilian who engages in actions tantamount to interference with military communications or operations through CNA (e.g., a Denial of Service operation) or CNE would constitute a DPCH attack in ICRC's view.

The Tallinn Manual thus incorporates the ICRC's notion by stating that:

[T]he act (or a closely related series of acts) must have the intended or actual effect of negatively affecting the adversary's military operations or capabilities, or inflicting death, physical harm, or material destruction on persons or objects protected against direct attack (threshold of harm).⁴³

The CCD COE experts provide that a cyber-attack that satisfies the "threshold of harm" is an operation that is reasonably expected to cause injury or death to persons or damage or destruction to objects.⁴⁴ The CCD COE was very specific that this "limitation should not be understood as excluding cyber operations against data (which are non-physical entities) from the ambit of the term attack."⁴⁵ This is especially true if an operation against data upon which the functionality of physical objects relies can sometimes constitute an attack.⁴⁶

However, for the purposes of DPCH against military adversaries, the CCD COE clarifies that there is no requirement for physical damage to objects or harm to individuals so long as a cyber-attack negatively affects enemy military operations.⁴⁷ For example, a cyber-attack that disrupts the operation of the military's command and control network would satisfy the criterion.⁴⁸ Disruption in this context does not mean physical damage to servers, data, or computers. Rather, it simply implies interference, no different from radio or radar jamming. This proposition is consistent with the ICRC's view under DPH. Stated negatively, if these actions were not directed at an adversary's military capability, the ICRC requires that the "specific act must be likely to cause at

information systems or networks." See Joint Terminology for Cyberspace Operations, *supra* note 37, at 3-4.

⁴² Skype Interview with cybersecurity strategist Joshua Corman, Chief Technology Officer at Sonatype (Sept. 23, 2013) (video recording on file with author).

⁴³ TALLINN MANUAL, *supra* note 5, at 119.

⁴⁴ *Id.* at 107.

⁴⁵ *Id.* at 107-08.

⁴⁶ *Id.* at 119.

⁴⁷ *Id.*

⁴⁸ *Id.*

least death, injury, or destruction” of property in order to reach this threshold of harm.⁴⁹ Thus, the ICRC’s notion as applied to CW means that a civilian hacker interfering with a civilian computer system (e.g., Social Security), instead of the military, would not necessarily lose protection for that purpose unless it can be demonstrated that either the cyber-attack against the non-military network was intended to have an effect on the military in some fashion or that physical harm would otherwise result.

As an aside, this notion of physical harm to a non-military network need not be defined in the physical destruction associated with a kinetic strike. An emerging trend is to define physical harm in the cyber domain as the level of effect on the functionality of the targeted object.⁵⁰ Some experts argue that if a cyber-attack impairs the functionality such that physical components require replacement, then this would constitute damage as envisaged in the concept of attack.⁵¹ Other experts provide that physical component replacement is not required; loss of functionality through data corruption requiring software re-installation or network rebooting would constitute “physical damage.”⁵² While the physical damage standard is not required for military networks, understanding this disparity is important if cyber-attacks against non-military networks occur as part of greater campaign during an armed conflict.

B. Direct Causation

The ICRC guidance provides that there must be a direct causation from the civilian act to the harm suffered for the act to potentially constitute DPH.⁵³ In particular, the ICRC states: “there must be a direct causal link between a specific act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part.”⁵⁴ In terms of a physical context, this implies that the harm suffered cannot be the result of an indirect or secondary order effect. The Tallinn Manual aligns with the ICRC’s DPH analysis by requiring the existence of “a direct causal link between the act in question and the harm intended or inflicted.”⁵⁵ In CW, this standard appears easier to fulfill than in the physical combat scenario, where “fog of war” tends to complicate the issue. By analogy, if a civilian farmer fires his weapon at another local national to ward off livestock poaching, the sound of gunfire or the physical impact of a bullet may incite a nearby military patrol to

⁴⁹ ICRC DPH GUIDANCE, *supra* note 23, at 49.

⁵⁰ Droege, *supra* note 11, at 557–58.

⁵¹ TALLINN MANUAL, *supra* note 5, at 108.

⁵² *Id.* at 109.

⁵³ ICRC DPH GUIDANCE, *supra* note 23, at 50–51.

⁵⁴ *Id.* at 51.

⁵⁵ TALLINN MANUAL, *supra* note 5, at 119.

engage in self-defense. In some instances, mere possession and public display of personal weapons, could be perceived as a threat without additional accompanying acts.

On the other hand, CW will not suffer from the same “fog of war” issue. The use of a cyber-weapon to deny a military’s capability or interfere with a military operation can hardly be seen as incidental or an indirect cause.⁵⁶ The Tallinn Manual supports this point through the example of disruption to the enemy’s command and control as being directly caused by a cyber-attack.⁵⁷ Therefore, if a civilian hacker gained access into a military network to exploit or disrupt the network, that civilian’s acts would be the direct cause of the harm suffered, rendering him or her targetable. As a counterpoint, this theory should not discount the possibility of accidental cyber-attacks by civilian entities or individuals. There are potential scenarios where technology companies or independent contractors could theoretically accidentally release malware onto a network. However, the Tallinn Manual and ICRC guidance on direct causation does not address the underlying intentions behind the action. Thus, the challenge with these scenarios is that they reinforce the notion of reasonable precautions within IHL (i.e., the obligation to take reasonable precautions to avoid or minimize incidental civilian losses).⁵⁸ Therefore, while fog of war is relatively diminished, prior to responding to a cyber-attack premised upon DPCH, reasonable precautions (e.g., reviewing human, electronic, and signals intelligence; verifying the source of the attack; using the least destructive means available to neutralize the threat) should be taken to minimize potentially attacking an otherwise innocent party.⁵⁹

C. Belligerent Nexus

The ICRC DPH guidance provides that:

In order to meet the requirement of belligerent nexus, an act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another.⁶⁰

⁵⁶ *Id.* at 119–20.

⁵⁷ *Id.* at 120.

⁵⁸ Additional Protocol I, *supra* note 4, art. 57(1); *see also Customary IHL—Rule 15. Precautions in Attack*, INT’L COMM. OF THE RED CROSS, http://www.icrc.org/customary-ihl/eng/docs/v1_cha_chapter5_rule15 (last visited July 30, 2014) (suggesting that Article 13(1) of Additional Protocol II implies this obligation); TALLINN MANUAL, *supra* note 5, at 164–65.

⁵⁹ *See generally* TALLINN MANUAL, *supra* note 5, at 159–176 (Rules 51–58).

⁶⁰ ICRC DPH GUIDANCE, *supra* note 23, at 58.

Hostile acts such as firing a weapon at an enemy or planting a bomb serve as easy examples. As a qualifying statement, the ICRC notes that acts that do not satisfy the threshold of harm are “non-belligerent . . . and, therefore, must be addressed through law enforcement measures.”⁶¹ A seminal example is the IED maker whose actions contribute to hostilities without necessarily being connected to the conflict. In this example, if the intelligence shows that the IED maker is developing and supplying bombs for the insurgents as a part of an ongoing campaign, then he/she is targetable. This analysis will change if he/she is just selling them to the insurgents. The ICRC also provides that the belligerent nexus element does not require a subjective intent determination, where the state of mind of the person is at issue in committing the act.⁶² The ICRC posits that a belligerent nexus requires an objective standard expressed in the design of the act or operation which does not depend on the mindset of every participating individual.⁶³ Belligerent nexus is generally not influenced by factors such as personal distress or preferences, or by the mental ability or willingness of persons to assume responsibility for their conduct. Consequently, if an insurgent is forced or coerced in some manner to commit an attack, he/she would still be lawfully targetable under IHL.

As applied, the Tallinn Manual expounds on the ICRC’s belligerent nexus notion by stating that cyber acts must be directly related to the hostilities between parties to a conflict.⁶⁴ By example, if a civilian directs a cyber-attack against a military’s command and control node, his or her actions would satisfy this condition as it impacts a military force to the benefit of the opposition. Equally, if a hacker were coerced to commit this cyber-attack, he or she would lose protection and become lawfully targetable. The Tallinn Manual’s criterion rules out acts of a purely criminal or private nature that occur during an armed conflict.⁶⁵ For example, hackers, using cyber means to commit a variety of crimes against non-military institutions, would not be targetable even if the victim State were a party to the conflict.⁶⁶ However, if the criminal actions were conducted to support particular military operations of one party and to the detriment of the military opposition, then the civilian would forfeit protection for DPCH.

⁶¹ *Id.* at 59.

⁶² *Id.*

⁶³ *Id.*

⁶⁴ TALLINN MANUAL, *supra* note 5, at 119.

⁶⁵ *Id.* at 120.

⁶⁶ *Id.*

IV. As Applied: Which Civilians are Targetable?

Given these cumulative factors, consideration should be given as to the categories of civilians who become lawful targets under DPCH. Up front, government-employed or -contracted computer technicians and related personnel would not be targetable under Geneva Convention III (GC III) as “persons who accompany the armed forces without actually being members thereof,” provided they fulfill more support roles and do not directly participate in hostilities.⁶⁷ On the other hand, if government contracted personnel were to engage in cyber hostilities, they would lose protection analogous to mercenaries.⁶⁸ Similarly, civilians who serve a continuous combat function in an organized armed group during an IAC or NIAC are targetable.⁶⁹ At a minimum, the Tallinn Manual’s guidance provides that members of organized armed groups, whether as levée *en masse* or not, who directly participate in hostilities, are targetable.⁷⁰ Such civilians will remain targetable throughout the conflict, including the temporal breaks in between or after attacks mentioned *supra*. However, the CCD COE experts remain divided over this issue. Some experts argue that a civilian who is simply a member of the group is targetable regardless of their nature, no differently from members of a uniformed armed force (with exception for protected clergy and medical personnel); others follow the ICRC DPH guidance requirement of a “continuous combat function.” Thus, a cook or administrative clerk for a non- state cyber-combat organization would not be targetable under the ICRC standard. This issue remains unresolved in the physical domain and will be resolved through policy or rules of engagement (ROE) decisions by leaders on a fact-specific basis. Nevertheless, civilians will be more readily targetable if they are part of a hostile group actively partaking in the armed conflict.

Notwithstanding these preliminary categories, identifying a civilian directly participating in cyber hostilities will be fact-specific and require a case-by-case analysis consistent with the principles discussed in Part III. Using these cumulative factors, the examples below illustrate the Tallinn Manual’s principles applied to unaffiliated civilians who directly participate in cyber hostilities. While not exhaustive, these examples serve as possible permutations for illustrating DPCH analysis via the Tallinn Manual and the ICRC’s DPH guidance.

⁶⁷ Art. 4(A)(4), Geneva Convention (III) Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 75 U.N.T.S. 135. *See also* Turns, *supra* note 8, at 292–93.

⁶⁸ TALLINN MANUAL, *supra* note 5, at 116–117.

⁶⁹ *Id.* at 116.

⁷⁰ *Id.* at 117.

A. Example One: The Case of the 13-year-old Thrill Seeker⁷¹

Civilians who are not parties to an IAC or NIAC may be lawfully targeted where they directly participate in cyber hostilities. Consider the hypothetical situation where, during an IAC between the U.S. and Iran, a 13-year-old child is armed with a laptop and malware. In this scenario, this hacker perpetrates a cyber-attack from Switzerland that is designed to disrupt a U.S. military logistics system related to moving of supplies and personnel for the purposes of disrupting (but not physically damaging) processes. This is especially conceivable given the inexpensive nature of developing or acquiring malicious code.⁷² Just recently a 12-year-old pled guilty to charges in Canada for hacking government systems in support of the international network of hacktivists known as Anonymous.⁷³

Once this hypothetical 13-year-old child conducts a cyber-attack by transmitting malware into this U.S. military logistics system, the child has clearly forfeited protection and is targetable for the following reasons: first, this act qualifies as an attack given that it meets the threshold of harm by disrupting military operations, where physical harm is not required;⁷⁴ secondly, the child's act of launching the malware directly causes the subsequent disruption (or attempted disruption);⁷⁵ lastly, the child's act satisfies the belligerent nexus element because the hostile act is directed against the U.S. military network and objectively benefits Iran.⁷⁶ Thus, the 13-year-old hacker is a lawful military target under a DPCH theory consistent with the ICRC and Tallinn Manual. Assuming the child only gained access to the network to exploit information by posting it to the internet, the child would still be targetable because such an act would exploit a vulnerability to the benefit of Iran. Conversely, if the child's actions were directed at a U.S. banking network, then the child's actions would be considered a criminal matter, unless the intelligence demonstrates that the child's actions were connected to the exploitation of U.S. infrastructure vulnerabilities in support of Iran's military campaign.

⁷¹ Emily Crawford, *Virtual Battlefields: Direct Participation in Cyber Warfare*, 9 ISJLP 1, 15 (2013), available at <http://moritzlaw.osu.edu/students/groups/is/files/2013/08/5-Crawford.pdf>.

⁷² Daniel Cohen & Aviv Rotbart, *The Use of Code Mutation to Produce Multi-use Cyber Weapons*, THE INSTITUTE FOR NATIONAL SECURITY STUDIES (Jul. 8, 2013), <http://www.inss.org.il/index.aspx?id=4538&articleid=5163>.

⁷³ Lisa Vaas, *12-year-old Canadian Boy Admits to Hacking Police and Government Sites for Anonymous*, NAKED SECURITY (Oct. 26, 2013), <http://nakedsecurity.sophos.com/2013/10/26/12-year-old-canadian-boy-admits-to-hacking-police-and-government-sites-for-anonymous/>; David Kushner, *The Masked Avengers, How Anonymous Incited Online Vigilantism from Tunisia to Ferguson*, THE NEW YORKER (SEP. 8, 2014), <http://www.newyorker.com/magazine/2014/09/08/masked-avengers>.

⁷⁴ TALLINN MANUAL, *supra* note 5, at 119.

⁷⁵ Turns, *supra* note 8, at 295.

⁷⁶ *Id.*

B. Example Two: Hacktivist⁷⁷

Patriotic hacktivism adds a different dimension to DPCH given that their activities may or may not cross the threshold of harm or have a nexus to the conflict. Russian hacktivists participated in a myriad of activities in Estonia in 2007 and Georgia in 2008.⁷⁸ Similar to the above example, a hacktivist, who disrupts military networks through distributed denial of service (DDoS) attacks, is targetable regardless of his or her subjective underlying intent. However, the analysis will change depending on whether their activities disrupt military operations. Suppose during this U.S.–Iranian conflict, a hacktivist from Anonymous decides to deploy a conspicuous message on a high-traffic, non-DoD, U.S. Government website as a form of cyber-protest of the war. While criminal, these actions will not constitute DPCH if the hacker’s actions do not have a belligerent nexus to the conflict, directly cause disruption to military operations, or cause physical harm. This scenario would be true if the hacktivist’s actions were targeted against the Affordable Care Act or Department of Justice websites.⁷⁹

On a sliding scale, the analysis changes if the hacker leaves a conspicuous message on a DoD information website as a form of “cyber-protest” of the war. An analysis of those actions is required to determine if the message interferes or disrupts military operations in order to satisfy the belligerent nexus requirement (supporting Iran). For example, if it could be determined that the message was designed to undermine the morale of DoD users fighting the war or interfere with military members’ readiness (e.g., disrupting military members’ pay on the Defense Finance and Accounting Service website), the hacktivist is clearly targetable under LOAC. However, if a hacktivist’s message or action cannot be readily connected to the conflict, he or she is still “at risk of being targeted, as their attacks would be difficult to differentiate from attacks being conducted by persons with a connection to the hostilities.”⁸⁰

C. Example Three: Malware Programmer⁸¹

Other roles, such as a malware programmer, are more complex to analyze for DPCH purposes because of the question of direct causation, no different from a weapons builder. Returning to the example of the U.S.–Iran conflict, a cyber-weapons programmer could have played a role in developing

⁷⁷ *Id.* at 293.

⁷⁸ *Id.* at 293, n.59.

⁷⁹ TALLINN MANUAL, *supra* note 5, at 119–20.

⁸⁰ Crawford, *supra* note 71, at 17.

⁸¹ *Id.* at 16; *see* Turns, *supra* note 8, at 295.

and providing the malware to the 13-year-old hacker. Whether the programmer is targetable depends on the nature of his or her involvement in supporting the hacker. According to the Tallinn Manual, if the programmer had specifically designed the malware for exploitation of a DoD vulnerability (e.g., a military logistics or finance website), then the malware programmer can be targeted. In this instance, the malware programmer's acts (designing a code to exploit a DoD vulnerability) directly cause the disruptive harm to the military's operations, directly benefiting Iran. Thus, the programmer can be lawfully engaged in addition to the 13-year-old executing the code.⁸² By analogy, an IED developer who designs bombs specifically to exploit U.S. military vehicles (e.g., up-armored HUMVEEs or MRAPs) is targetable under DPH.

Conversely, if the malware programmer's only activity is developing generalized malware made available on a website, then causation would not be satisfied given the remoteness of involvement.⁸³ This permutation resembles someone ordering firearms from an online vendor. An online vendor of cyber weapons does not become targetable, unless it is demonstrated that this developer is selling specialized malware to undermine DoD systems during an armed conflict. On the other hand, if the programmer designs malware for the 13-year-old, unaware of the intended target, there may be two possible outcomes.⁸⁴ The CCD COE members were divided on malware programmers in this scenario.⁸⁵ Drawing from the analogy of an IED builder, if military intelligence can establish factors supporting the inference that malware is specifically designed to exploit military weaknesses, then the programmer is targetable, unlike a person developing Trojan Horse viruses downloadable via a website. In short, further targeting decisions of malware programmers will require additional indicia of direct causation.

D. Technical Support Personnel⁸⁶

As a final example, technical support personnel require consideration under a DPCH analysis. If the 13-year-old hacker solicits technical support, the nature of that individual's involvement will be a determining factor for DPCH. If the hacker contacts technical support to assist with hardware or system software issues pertaining to the computer, then the support personnel will not be targetable as they are neither connected to the conflict nor the direct cause of harm.⁸⁷ This result would be the same if the technical personnel assisted with

⁸² Turns, *supra* note 8, at 295.

⁸³ TALLINN MANUAL, *supra* note 5, at 120.

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ Crawford, *supra* note 71, at 17.

⁸⁷ *Id.*

hardware and software issues knowing the intentions of the hacker.⁸⁸ These personnel are criminally liable for such actions under a domestic framework within the United States, but are not targetable under LOAC. On the other hand, if a malware programmer provides technical assistance or instructive guidance to the child hacker on refining malware to exploit DoD systems, then the programmer (as a technical advisor) would lose their protected status and be targetable consistent with the Tallinn Manual's view of a DPCH framework.

V. Challenges

The cumulative criteria mentioned above provide only a starting point for understanding what actions render a civilian targetable under LOAC. The decision to use force against a non-state civilian actor who directly participates in hostilities raises a myriad of other issues that will require consideration by states engaged in armed conflict. Each topic is individually complex and could be explored in elaborate discussions beyond the scope of this article. Nevertheless, the below discussions are limited to understanding how a state should consider these issues prior to considering a response to a civilian who forfeits protection under DPCH. These scenarios assume that the non-state actor's attacks are not attributable to the state.

A. Sovereignty

"Longstanding notions of sovereignty fall apart when it comes to cyber operations."⁸⁹ This quote foretells of a complex predicament should neutral nations become the staging grounds for non-state actors launching cyber-attacks in either IACs or NIACs. Of equal importance, the manner in which a State responds to civilians participating in CW from outside the theater of hostilities presents a challenging issue given that such neutral States maintain the inherent right of self-defense pursuant to Article 51 of the U.N. Charter.⁹⁰ For IACs, LOAC provides that belligerent nations are prohibited from actions that harm a neutral nation and draw it into the conflict in any fashion.⁹¹ Conversely, neutral

⁸⁸ *Id.* at 18.

⁸⁹ Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 *FORDHAM INT'L L.J.* 815, 816 (2012) (citing David Perera, *Schmidle: Cyber Ops Might Require New Combatant Command Structure*, *FIERCEGOVERNMENTIT* (May 15, 2011, 4:29 PM), <http://www.fiercegovernmentit.com/story/schmidle-cyber-ops-might-require-newcombatant-command-structure/2011-05-15> (quoting Lieutenant General Robert Schmidle, Deputy Commander of US Cyber Command)).

⁹⁰ *Id.*; see also UN Charter art. 51.

⁹¹ Jensen, *supra* note 89, at 819; see also INT'L COMM. OF THE RED CROSS, *THE LAW OF ARMED CONFLICT: LESSON 8: NEUTRALITY* (2002), available at http://www.icrc.org/eng/assets/files/other/law8_final.pdf ("The sources of the international law of neutrality are customary international law and, for certain questions, international treaties, in particular the Paris Declaration of 1856, the 1907 Hague Convention No. V respecting the Rights

nations have an obligation to maintain neutrality by preventing actions within their territories that cause harm to a party to a conflict.⁹² While it is arguable that the law of neutrality does not extend to NIACs, the international law principle of *sic utere* provides that a state cannot knowingly allow its territory to be used to the detriment of another.⁹³ Moreover, as illustrated in the *Nicaragua v. United States*⁹⁴ case, the International Court of Justice (ICJ) supported the proposition that states engaged in non-international conflict enjoy a right of non-interference from outside parties.⁹⁵

To illustrate, suppose the non-state actor sponsored 13-year-old hacker launches a cyber-attack against the United States from Switzerland in support of Iran. Notwithstanding the existence of an extradition treaty, Switzerland has had a history of harboring U.S. fugitives.⁹⁶ In this scenario, suppose also that the United States locates and identifies the attacker. If the Swiss preclude this individual from attacking further but refuse to extradite, then the United States would no longer be able to target this individual under the temporal considerations of a LOAC analysis. Alternatively, if the Swiss take no action at all or are unable to prevent harm from occurring, then the United States would find itself in a predicament that theoretically draws a comparison of physical terrorist attacks launched from lawless countries, including (pre-9/11) Afghanistan or Somalia.⁹⁷ Thus, the United States can launch a non-kinetic

and Duties of Neutral Powers and Persons in Case of War on Land, the 1907 Hague Convention No. XIII concerning the Rights and Duties of Neutral Powers in Naval War, the four 1949 Geneva Conventions[,] and Additional Protocol I of 1977. The United Nations Charter of 1945 and Security Council decisions based on the Charter may in certain circumstances modify the law of neutrality. For example, Article 2(5) of the Charter requires UN Member States to give the UN every assistance in any action it takes, and Article 25 requires UN members to accept and comply with the decisions of the Security Council; the enforcement measures spelled out in Chapter VII can also have an impact, as they are governed by particular rules which differ from those of the law of neutrality.”).

⁹² Jensen, *supra* note 89, at 819.

⁹³ Jutta Brunnée, *Sic utere tuo ut alienum non laedas*, in 9 MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 188 (2012); See also Jack Goldsmith, *Thoughts on the Latest Round of Johnson v. Koh*, LAWFARE (Sept. 16, 2011, 8:43 AM), <http://www.lawfareblog.com/thoughts-latest-round-johnson-v-koh> (“If the president is authorized to use force against a terrorist group by Congress, and if the U.N. Charter’s sovereignty concerns are overcome because the nation in question is unwilling or unable to address the group’s threat to the United States, and as long as the United States complies with *jus in bello* restrictions on targeting (distinction, proportionality, etc.), there is no further legal requirement.”).

⁹⁴ Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27).

⁹⁵ *Id.* at 181 (separate opinion of Judge Ago).

⁹⁶ Andrew Henderson, *The Best Non-extradition Countries to Become Invisible*, NOMAD CAPITALIST (June 3, 2013), <http://nomadcapitalist.com/2013/06/03/the-best-non-extradition-countries-to-be-invisible/>.

⁹⁷ Kevin J. Heller, *The “Unwilling or Unable” Standard for Self-Defense*, OPINIO JURIS (Sept. 17, 2011, 2:42 AM), <http://opiniojuris.org/2011/09/17/the-unwilling-or-unable-standard-for-self-defense-against-non-state-actors/>.

response against the server and computer in question. Moreover, the United States can target the 13-year-old kinetically for committing cyber-attacks against its military consistent with the cumulative factors under the Tallinn Manual's view.

Both responses would be proffered as an "unwilling or unable" international law argument.⁹⁸ Although scholars support this standard's incorporation into customary international law, the ICJ rejected it on several occasions and thus, the "unwilling or unable" doctrine remains contentious and unsettled within customary international law (CIL).⁹⁹ Should the United States invoke this standard, as in the case of Afghanistan in 2002, a U.S. response without Switzerland's permission could result in strong political and military repercussions. Unlike Afghanistan before September 2001, Switzerland is not a lawless State, but still bears the responsibility under the *sic utere* doctrine to prevent international cyber-attacks from occurring within its national borders. In response to a U.S. kinetic or non-kinetic attack against the hacker, the Swiss could bring the issue to the ICJ. Switzerland could also respond militarily or in the cyber domain in self-defense against the United States. Given the permutations involved, this scenario illustrates the several considerations the United States would confront in conducting a counter-attack against a hacker located in a neutral State that refuses to cooperate.

B. Law of Targeting Considerations

If the United States responds to this hacker in the cyber or physical domain, "targeting law" will certainly apply in both cases. "Targeting law" evaluates whether the weapon's employment (methodology) would violate the general principles of LOAC.¹⁰⁰ The general principles of LOAC involve military necessity, distinction, proportionality, and humanity.¹⁰¹ For the purposes of kinetic operations using conventional means in the physical domain, targeting law remains well settled. As noted in the Tallinn Manual, these concepts do apply in the cyber domain and will require further examination. "Military necessity may be defined as the principle that justifies the use of all measures needed to defeat the enemy as quickly and efficiently as possible that are not prohibited by the law of war."¹⁰² Thus, military commanders must act in a manner necessary for advancing military objectives and ensure that their actions

⁹⁸ Goldsmith, *supra* note 93.

⁹⁹ *Id.*

¹⁰⁰ Jeffrey S. Thurnher, *The Law that Applies to Autonomous Weapon Systems*, 17 AM. SOC'Y INT'L L. INSIGHTS (Jan. 18, 2013), <http://www.asil.org/insights/volume/17/issue/4/law-applies-autonomous-weapon-systems>.

¹⁰¹ U.S. DEP'T. OF DEF., DOD LAW OF WAR MANUAL 50 (JUNE 2015).

¹⁰² *Id.* at 52. See also IAN HENDERSON, THE CONTEMPORARY LAW OF TARGETING 7 (2009).

are not otherwise prohibited by another principle of LOAC.¹⁰³ As a principle, military necessity not only tolerates violence towards the enemy but alternative operations which influence or impede the enemy (e.g. psychological operations, electronic jamming, intelligence operations).¹⁰⁴ As applied, cyber-attacks may be employed against military objectives provide such actions do not violate the principles of proportionality, humanity, and distinction.

“Humanity” implies that belligerents should not cause unnecessary suffering. The CCD COE posits that “[m]eans and methods of cyber warfare will only in rare cases violate this Rule.”¹⁰⁵ However, the Tallinn Manual illustrates a possible violation of this rule through hacking into a victim’s pacemaker to stop the target’s heart and then reviving him multiple times before finally killing him.¹⁰⁶ An example could include hacking into pharmaceutical records for the purpose of prescribing medications aimed at causing long-term allergic reactions leading to death. Using a cyber-attack to poison or corrupt a military water supply serves as another example as strictly prohibited as a violation of this LOAC principle. Given the ramifications, U.S. policy would exclude attacking this hacker through means that cause unnecessary suffering.

As mentioned earlier, “distinction” requires combatants to distinguish between lawful military targets (opposing combatants and their equipment and facilities) and protected persons (e.g., civilians, medical personnel, chaplains, hors de combat) and property. However, in DPH and DPCH targeting contexts, distinction requires discriminating between civilians who have forfeited protection from those civilians and related objects that retain protection. Thus, if the United States were to conduct a non-kinetic cyber-attack against the 13-year-old hacker via a Swiss server, the United States would need to utilize malware that targets the offending computer only with no adverse effect or corruption of the server or other resident users. Similarly, if the 13-year-old hacker were using a Wi-Fi café in a Swiss hospital, the United States would not be able to attack the hospital’s server given that it is protected. If the United States can transmit a response (e.g., a DDoS attack) through the Wi-Fi café router that only impacts the targeted computer, then distinction would be otherwise satisfied. Similarly, targeting servers for non-kinetic (e.g., DDoS) or kinetic (e.g., Stuxnet-type virus) purposes requires verification of the hacker’s location. Therefore, the United States would need intelligence models on the systems’ architects and servers in order to modify malware to distinguish civilian perpetrators from protected persons.

¹⁰³ *Id.* at 52.

¹⁰⁴ *Id.* at 53.

¹⁰⁵ TALLINN MANUAL, *supra* note 5, at 144.

¹⁰⁶ *Id.*

Traditionally, the term civilian objects implied buildings, utilities (e.g., power lines), and related infrastructure. For cyber considerations, civilian objects would include such items as servers, computers, and related hardware. Data is also considered a protected object, especially if the data on a resident server is owned by a protected civilian. As mentioned, the CCD COE specifically chose not to exclude data from the ambit of the term “attack.” This is especially true where malware is directed against data that physical objects rely upon for functionality.¹⁰⁷ Thus, a cyber-attack that damages protected civilian data would violate the rules of distinction. While the data’s restoration via a backup could serve as a test for targeting, this is not the test used for physical property since buildings can be rebuilt, and cars can be remanufactured over time. Thus, this issue remains unsettled and a consideration for distinction. As applied, if the Wi-Fi café shares the same servers which contain patients’ records and data, then the intentional damage to such data would violate this principle.

Targeting law also requires a “proportionality” analysis.¹⁰⁸ The Tallinn Manual restates the requirements for proportionality codified in customary international law and in AP I:

A cyber[-]attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited.¹⁰⁹

While this principle is simply stated, proportionality is entirely subjective given that comparing the value of a military advantage to damage to civilians is tantamount to comparing “apples to oranges.”¹¹⁰ The analysis becomes case-specific, based on the nature of the target and the national thresholds for collateral damage. As applied, if the United States decides to conduct a DDoS attack against the 13-year-old hacker in Switzerland in a hospital Wi-Fi café, then the United States will have to assess the effects of the DDoS attack on that network and whether the resultant collateral damage can be mitigated by modifying the malware.¹¹¹ By comparison, such modifications are consistent with DoD Collateral Damage Estimation Methodologies (CDEM) for

¹⁰⁷ *Id.* at 108, 113.

¹⁰⁸ HENDERSON, *supra* note 102, at 7.

¹⁰⁹ TALLINN MANUAL, *supra* note 5, at 159 (Rule 51).

¹¹⁰ KENNETH ANDERSON & MATTHEW WAXMAN, LAW AND ETHICS FOR AUTONOMOUS WEAPON SYSTEMS: WHY A BAN WON’T WORK AND HOW THE LAWS OF WAR CAN 12 (2013), available at <http://www.hoover.org/publications/monographs/144241>.

¹¹¹ TALLINN MANUAL, *supra* note 5, at 113.

conventional weapons so as to avoid malware collaterally spreading or damaging other users, data, or networks.¹¹² An analysis of the Stuxnet malware revealed fail-safe features such as code that limited the infection to Siemens systems, the number of devices that each infected device could infect, and the self-destruct code erasing the virus on June 24, 2012.¹¹³ Regardless of the overall effectiveness of the fail-safe measures, they illustrate “the inherent caution” of Stuxnet’s creators as an attempt to prevent further damage to other systems.¹¹⁴ Nations attempting to develop more sophisticated cyber weapons will need to consider proportionality issues and collateral damage.

VI. Practical Responses to Civilians who Directly Participate

Despite challenges associated with cyber-warfare, States have a right of self-defense against civilians who conduct cyber-attacks during an armed conflict setting. While political and diplomatic measures remain available, the foregoing discussion provides an understanding of the nature of each response to a DPCH scenario assuming the offending civilian is located and attributed to the action. For the purposes of this framework, the U.S.–Iran armed conflict scenario discussed earlier will be utilized again.

A. Non-kinetic Responses

Non-kinetic response can be acknowledged or covert as discussed below. Cyber defenses, for example, can be employed to have a non-kinetic effect depending upon their intended effect and usage. If a hacker attempts to gain access into an otherwise prohibited system, the host system can utilize a defense that can essentially block such access with no further effect. More active cyber defenses include tracking hackers’ computers, hacking back into systems to retrieve data, shutting down systems, sabotaging data, infecting the attacker with malware, taking over the attacker’s botnet, or employing a botnet to track or attack the hacker’s computer.¹¹⁵ While active defense responses to DPCH seem plausible, LOAC principles must be taken into consideration. For instance, if a DoD system conducts an active defense hack-back or counter-attack using

¹¹² CDEM assesses the likelihood of collateral damage for conventional weapons based on several factors, such as types of weapons, employment tactics, proximity of civilian structures. *See generally* Major Jefferson D. Reynolds, *Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground*, 56 A.F. L. REV. 1 (2005).

¹¹³ Michael J. Gross, *Stuxnet Worm: A Declaration of Cyber-War*, VANITY FAIR (Apr. 2011), <http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104>.

¹¹⁴ *Id.*

¹¹⁵ Jody Westby, *Caution: Active Response to Cyber Attacks Has High Risk*, FORBES (Nov. 29, 2012, 10:52 AM), <http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/>.

malware, such programs must be capable of limited or no effects on innocent users or servers. A more interesting question is how such systems can distinguish between a criminal hacker and a LOAC hacker. At a minimum, in both cases, employing an active defense capable of preserving evidence and intelligence related to this hacker and operation will be critical for potential prosecution or follow-on responses.¹¹⁶ Offensive cyber capabilities with non-kinetic effects would employ similar effects described for active defenses. The distinction is that offensive capabilities would not necessarily occur as an automatic response from a computer, but rather a directed operation.

B. Kinetic Responses

Responding to a cyber-attack kinetically raises questions regarding escalation. A response can take on two forms: a conventional attack (e.g., a missile) or a cyber-attack with physical effects (e.g., Stuxnet). Due to political and diplomatic considerations, use of force by the United States will require nothing short of Presidential authorization. In the instance of international armed conflict, the legal framework for employing a kinetic attack against a designated hostile force or individual (e.g., via AUMF or “targeted killing”) is well settled.¹¹⁷ A cyber-attack with kinetic effects directed against designated hostile forces in a theater of combat is legally supportable. Similarly, the targeted killing of a U.S. terrorist in self-defense is also considered consistent with U.S. domestic law, whether conducted with a drone strike or a kinetic cyber-attack. As scholar Hays Parks notes, the targeted killing of a legitimate enemy is not assassination.¹¹⁸ If a civilian forfeits protection due to DPCH attacks or serves as a cyber-terrorist causing physical harm to U.S. civilians, he or she can be lawfully targeted with a kinetic attack. With this understanding, there will be some additional considerations.

If the 13-year-old hacker is in Iran during the U.S.–Iranian conflict, the United States could escalate to kinetic force against the child no differently from an insurgent planting IEDs or shooting at a military convoy. On the other hand, kinetic operations during a cyber-only conflict expand the range of options available to the hostile nation for targeting a civilian cyber-attacker within its borders.¹¹⁹ In other words, Iran would be able to escalate to kinetic force in self-defense. Thus, in a cyber-only conflict, targeting this hacker kinetically may

¹¹⁶ *Id.*

¹¹⁷ *US to Outline Legal Backing for ‘Targeted Kill’ Programme*, THE GUARDIAN (Mar. 1, 2012, 2:58 AM), <http://www.theguardian.com/world/2012/mar/05/us-legal-backing-targeted-kill-programme>.

¹¹⁸ W. Hays Parks, *Memorandum of Law: Executive Order 12333 and Assassination*, ARMY LAW., Dec. 1989, at 4.

¹¹⁹ Herbert Lin, *Escalation Dynamics and Conflict Termination in Cyberspace*, STRAT. STUD. Q. 46, 65 (2012).

undoubtedly escalate the conflict and requires political considerations. These considerations are heightened if kinetic force is applied to or within neutral nations as mentioned in Part IV. A kinetic response to a cyber-attack will require a case-by-case analysis of the nature of the cyber-attack's operation, intended target(s), and underlying strategic significance.¹²⁰ At a minimum, kinetic action, whether conducted through conventional or cyber-attacks, should be limited in scope and duration, consistent with self-defense proportionality principles, in order to avert an unnecessary escalation.

C. Covert Action

In most cases, the benefit of acknowledged non-kinetic or kinetic cyber-attacks against a neutral nation will be significantly outweighed by the diplomatic, economic, and military backlashes that would occur. Such acts would undoubtedly be perceived as an act of aggression by the United Nations, as interpreted by the ICJ.¹²¹ For these reasons, covert action represents a readily available solution while CIL develops in this area. Responding to non- state actors performing cyber-attacks from neutral states presents complex issues given the potential of affronting neutrality and widening the conflict. The stealthy nature of cyber warfare enables covert action as use of the cyber domain enables anonymity, takes advantage of targeted individuals' awareness, and utilizes speed that overcomes the ability to readily safeguard against the consequences.¹²² Returning to the earlier scenario involving the child hacker located in Switzerland, the United States could consider covert action to thwart this non- state actor. This scenario presumes that Switzerland is uncooperative in extraditing or precluding this child from committing cyber-attacks against the United States.

First, the United States could consider a targeted killing operation against this individual within Swiss borders. The targeting of this child for DPCH in support of Iran would not be considered an assassination as prohibited by Executive Order 12333.¹²³ Under U.S. domestic law, an Authorization to Use Military Force will be required to authorize targeted killings. This requirement was illustrated in the U.S. campaign against al-Qaeda. Assuming the U.S.–Iranian conflict contains an AUMF, language should be included to at least authorize the killing of supporting parties for DPCH, regardless of location. This

¹²⁰ *Id.* at 61.

¹²¹ See generally UN Charter, arts. 2(4), 51; see also *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, 181 (June 27) (separate opinion of Judge Ago); Jensen, *supra* note 89, at 821.

¹²² Ellyne Phneah, *Cyber Warfare Not Theoretical, Can Actually Kill*, ZDNET (Nov. 17, 2011, 5:26 AM), <http://www.zdnet.com/cyber-warfare-not-theoretical-can-actually-kill-2062302921/>.

¹²³ Parks, *supra* note 118.

proposition would provide legal credibility since Executive Order 12333 prohibits the unlawful, politically-motivated killing of a person who is not a legitimate target. Alternatively, even if an AUMF does not have broader language, a covert targeted killing would still be lawful if it can be established that the killing was required in self-defense consistent with Article 51 of the UN Charter. To prevent attribution of such killing within Swiss borders, the United States could use military means, such as Special Forces operations analogous to those employed during the Osama bin Laden raid.

Second, covert action could also be conducted for rendition of the child to prosecute him in the United States. The practice of rendition (also referred to as irregular rendition) is typically defined as the kidnapping or taking of an individual to move that person to the jurisdiction of another country.¹²⁴ This is distinguished from extraordinary rendition which involves transferring the individual to a foreign country for the purposes of detention and interrogation by a foreign government.¹²⁵ Rendition does not deprive U.S. courts of jurisdiction unless an applicable extradition treaty explicitly calls for that result and that treaty has been given legislative effect within U.S. domestic law.¹²⁶ Since the U.S.–Swiss extradition treaty contains no rendition language, the United States would not be barred from exercising jurisdiction and prosecuting this individual.¹²⁷ A covert action for rendition would resemble a raid using either special operations or U.S. law enforcement.

Finally, covert action could be carried out against this individual via cyber means. A cyber-attack could have a non-kinetic or kinetic impact, as discussed earlier, and would be a more tenable solution if the originator of the attack were unknown. A covert operation employing cyber capabilities would require a complex number of variables beyond the scope of this article. Needless to say, such an operation would involve understanding the location of the child, a breakdown of the child's activities (pattern of life), an understanding of the targeted system's architecture, and other variables. A covert, non-kinetic cyber-attack could be aimed at locating, tracking, and denying access to the 13-year-old hacker via the child's computer or home internet service provider. This kind of non-kinetic operation could be aimed at developing further intelligence on the child's activities for further planning should the child continue his or her attacks.

¹²⁴ BARRY E. CARTER & ALLEN S. WEINER, INTERNATIONAL LAW 1086 (6th ed. 2011).

¹²⁵ *Id.* at 236.

¹²⁶ MICHAEL J. GARCIA & CHARLES DOYLE, CONG. RESEARCH SERV., EXTRADITION TO AND FROM THE UNITED STATES: OVERVIEW OF THE LAW AND RECENT TREATIES 33 (2010).

¹²⁷ Extradition Treaty, U.S.–Switz., Nov. 14, 1990, S. TREATY DOC. 104-9 (1997), available at <http://www.gpo.gov/fdsys/pkg/CDOC-104tdoc9/pdf/CDOC-104tdoc9.pdf>.

A covert kinetic cyber-attack could vary greatly. Malware could be used to destroy the child's data or to render the child's computer unusable. On the other hand, if the desired effect is to kill the 13-year-old hacker, then a more elaborate cyber-attack would be required. Should the child need a pacemaker or medical assistance, a potential attack would include using malware or other cyber technique to kill the hacker, provided that the prohibition against unnecessary suffering was enforced. "CyberJacking," the act of remotely taking control of someone's vehicle, could be used as cyber means of a targeted killing.¹²⁸ In this past summer's BlackHat conference, two researchers demonstrated how they could control a car using their laptop while within the car.¹²⁹ Such capabilities could easily be weaponized to target this 13-year-old hacker, assuming that the killing of the civilian driver or other occupants as collateral damage would be proportionally acceptable under the circumstances.

VII. Conclusion

In summary, DPCH will remain an ongoing concern in the coming years given the lack of an international consensus on the basic legal principles governing hostilities in the cyber domain. At a minimum, the Tallinn Manual's DPCH framework provides clear guidance derived from IHL that will enable states to respond to civilian hackers who undertake hostilities in armed conflict while seeking to prevent collateral damage. While developing a cyber-hostilities treaty appears as a readily available solution, the sharp disagreement among states (e.g., the United States, Great Britain, France, China, Russia) on the basic principle of regulating the cyber domain makes such treaty a fleeting prospect. Nevertheless, states always retain the inherent authority of self-defense, regardless of the lack of international consensus concerning cyber hostilities. Thus, IHL provides an immediate legal framework for cyber operations. Over time, these practices will refine and crystalize into customary international law through State practice and *opinio juris*. Although international consensus seems unattainable, regional or organization practices such as the NATO effort in the Tallinn Manual support the development of CIL in those regions. While the cyber domain requires an analysis of the nature of hostilities, the principles of IHL govern the conduct of these hostilities in order to safeguard against collateral damage while preserving a state's right of self-defense.

¹²⁸ Scott Schweitzer, *CyberJacking, Sophisticated Assassination*, CYBER WEAPONS & WARFARE (Oct. 6, 2013, 8:55 AM), <http://cyberweapons.blogspot.com/>.

¹²⁹ *Id.* The BlackHat conference is a yearly event where thousands of security experts gather to discuss information security and expose vulnerabilities at the pertaining to computers, networks and other related digital media. Megan Rose Dickey, *What Happens At 'Black Hat,' The World's Biggest Conference For Hackers In Las Vegas*, BUS. INSIDER, July 30, 2013, <http://www.businessinsider.com/what-happens-at-the-black-hat-conference-2013-7#ixzz3h3JLEqy>.

INVESTIGATING CIVILIAN CASUALTIES IN ARMED CONFLICT: COMPARING U.S. MILITARY INVESTIGATIONS WITH ALTERNATIVES UNDER INTERNATIONAL HUMANITARIAN AND HUMAN RIGHTS LAW

Commander Sylvaine Wong, JAGC, USN*

I. Introduction

Armed conflict since 11 September 2001 has seen a striking rise in the number of civilian casualties, despite the international commitment to minimizing the ravages of war on civilians following the Second World War. Coalition operations in Afghanistan have been no exception to this rise in casualties. In August 2010, the United Nations Assistance Mission in Afghanistan (UNAMA) issued its Mid-Year Report on Protection of Civilians in Armed Conflict,¹ finding that 3,268 civilians were killed or injured from January to June of that year—a 31 percent increase from a year prior. UNAMA attributed 76 percent of those casualties to the Taliban and allied groups (up 53 percent from 2009), and only 12 percent to international coalition and Afghan government forces (down 30 percent from 2009). Of that 12 percent, UNAMA found that the majority were the result of airstrikes by coalition forces.

Prior to 2009, although most of the individual casualty cases were tracked only by victims' families or local organizations, some incidents garnered significant

* The author is currently a Commander in the United States Navy, Judge Advocate General's Corps. Her previous duty assignments include the NATO International Security Assistance Force, Regional Command (South) in Kandahar, Afghanistan, and the Office of the Judge Advocate General of the Navy, Administrative Law Division, in Washington, DC. This article was written while enrolled as an LL.M. student at Harvard Law School during the 2010-2011 academic year. Special thanks to Professor Robert Sloane for providing guidance and substantive feedback on its draft, and Lieutenant Commander Bradley Davis for his significant assistance preparing this article for publication. The views and opinions expressed herein are those of the author and do not necessarily reflect the official positions of the Department of Defense or the Department of the Navy.

¹ UNITED NATIONS ASSISTANCE MISSION IN AFGHANISTAN (UNAMA), ANNUAL REPORT ON PROTECTION OF CIVILIANS IN ARMED CONFLICT, MID-YEAR REPORT 2010, August 2010 <http://www.unhcr.org/refworld/docid/4c6120382.html>.

local and international media coverage. They were notable not only for their high number of casualties but also the wildly varying accounts of what happened or how many were killed or injured. For example, Afghan reports of a 22 August 2008 airstrike in the village of Azizabad, Shindad District, Herat Province, alleged U.S. forces killed 90 civilians. After conducting a national investigation, the United States reported only seven civilians were killed.² On 4 May 2009, Afghan reports alleged an air strike by U.S. forces in Bala Boluk, Farah Province, killed 140 civilians. After the national investigation, the United States alleged 26 civilians were killed. In neither case were military forces found to have violated the law of armed conflict, although the latter case did lead the commander of U.S. and coalition forces in Afghanistan to issue a tactical directive placing restrictions on future air strikes in the country.³

A. The International Critique

Nations have traditionally borne ultimate responsibility for ensuring their own military conduct is in accordance with established international norms. For example, major national investigations examined the conduct of Canadian forces in Somalia in 1993, Dutch forces in Srebrenica in 1995, and American forces at Abu Ghraib Prison in Iraq in 2004. Subsequent to the investigations, Canadian and American military personnel were prosecuted under their respective national military justice systems, while the Dutch government resigned in 2002 as a symbol of accepting responsibility for the actions of its armed forces.⁴ But recent failures to find wrongdoing in major civilian casualty incidents have sparked human rights advocates to push for greater scrutiny of military forces through international investigations.

In the wake of the UNAMA report, Philip Alston, the U.N. Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions, recommended that civilian casualties caused by pro- and anti-government forces in the conflict in Afghanistan be investigated by the U.N. Human Rights Council (UNHRC).⁵ He stated, “If states are not carrying out reasonably neutral investigations and prosecutions of what appear to be serious violations, it does leave open the possibility that the international community should be intervening in some

² *Chronology, July 16, 2008 – October 15, 2008*, 63 MIDDLE EAST J. 1, 109 (2009).

³ See, e.g., Jason Motlagh, *U.S. to Limit Air Power in Afghanistan*, WASH. TIMES, June 24, 2009, <http://www.washingtontimes.com/news/2009/jun/24/us-to-limit-air-power-in-afghanistan/>.

⁴ See CHARLOTTE KU & HAROLD K. JACOBSON, *Toward a Mixed System of Democratic Accountability*, in DEMOCRATIC ACCOUNTABILITY AND THE USE OF FORCE IN INTERNATIONAL LAW 374 (Charlotte Ku & Harold K. Jacobson, eds., 2003).

⁵ Press Release, Office of the High Commissioner for Human Rights, Special Rapporteur Calls on the Government and the International Community to Make Renewed Efforts to Prevent Unlawful Killings (May 15, 2008) [hereinafter OHCHR], available at <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=8675&LangID=E>.

way.”⁶ Alston criticized existing national investigatory systems for their lack of transparency and accountability – especially with regard to those personally affected by the death of a loved one – while “the maze of overlapping mandates and multiple national systems of military justice”⁷ frustrates the overall search for accountability. He described the difficulty local Afghans had in ascertaining whether an investigation occurred into the death of a family member by a ground or air attack. Referring to the coalition’s stated need to gain the trust and confidence of the local populace in order to successfully carry out counterinsurgency operations, Alston proclaimed, “[family members] often come away empty-handed, frustrated and bitter. This is counter-productive and must end.”⁸

Alston’s critique echoed the call by Amnesty International 10 years earlier in its review of North Atlantic Treaty Organization (NATO) operations in Kosovo. Amnesty criticized the dearth of information provided by NATO about civilian casualty investigations – and the minimal disciplinary action and compensation that resulted – although it praised the U.S. investigative response in comparison. Specifically, it stated, “[t]he confidential nature of any investigation and the reported absence of measures against any NATO personnel cast doubt on NATO’s commitment to getting to the bottom of specific incidents in accordance with international law.”⁹ Calling for NATO to improve its investigation of international humanitarian law violations, Amnesty recommended NATO “[call] on the services of the International Humanitarian Fact-Finding Commission established under Article 90 of Protocol I The methods and findings of this investigation should be made public and used to assist any prosecution that may appear appropriate.”¹⁰

The United Nations has echoed these concerns on occasion. The 1996 Israeli shelling of a U.N. compound in Qana, Lebanon, killing more than 100 civilian refugees, prompted the U.N. Secretary General to immediately initiate his own investigation into the incident. Although Israel contended that the incident was not deliberate and was the result of faulty intelligence or equipment, its national investigatory process was discounted and the U.N.

⁶ See Mark Townsend, *Call for ‘Gaza style’ inquiry on Afghan deaths*, THE OBSERVER, Sept. 26, 2010 <http://www.guardian.co.uk/law/2010/sep/26/afghanistan-demand-war-crimes-probe>.

⁷ OHCHR, *supra* note 5.

⁸ *Id.*

⁹ AMNESTY INTERNATIONAL, “COLLATERAL DAMAGE” OR UNLAWFUL KILLINGS?: VIOLATIONS OF THE LAWS OF WAR BY NATO DURING OPERATION ALLIED FORCE, EUR 70/18/00, NATO/FRY, 23, 25 (June 2000) [hereinafter AMNESTY].

¹⁰ *Id.* at 28.

investigation concluded “it [was] unlikely that the shelling of the United Nations compound was the result of gross technical and/or procedural errors.”¹¹

B. Responding to the Critique

Although Alston refers to the transparency and accountability of the investigatory process, the distinction between the two notions is crucial. Accountability suggests the imposition and ultimately acceptance of legal responsibility, often through criminal prosecution, for military conduct that resulted in civilian casualties. Although critical, and subject to extensive discussion outside the scope of this paper, it is secondary to the immediate concern of the local populace. As Alston notes, the primary concern for family members is what happened to those who were killed and why they were killed. In this respect, the transparency of the investigation process itself is more critical, and the integrity of the fact-finding process precedes the outcome of the evaluation.

But despite the appeals to use the International Humanitarian Fact Finding Commission (IHFFC) to increase the transparency of investigations, the United States, one of the largest military forces in the world, continues to refuse to subject its troops to international scrutiny of this level. It is not legally obligated to do so, as it has never become party to Additional Protocol I. Many proponents in the U.S. system maintain that national investigations are sufficient to provide accountability of the conduct of its forces, despite the increasing number of civilian casualties. If human rights advocates hope to bring the United States within the cognizance of the IHFFC, they must identify the incentives for U.S. consent. This paper attempts to identify those incentives by systematically comparing the practical functioning of the existing national investigatory system with other international mechanisms. It highlights the benefits and potential pitfalls of each with respect to state obligations to investigate civilian casualty incidents.

Part I explores the legal requirements pursuant to international law and underlying principles for civilian casualty investigations in armed conflict. Two normative frameworks—international humanitarian law (IHL) and human rights law—establish the scope of a state’s duty to investigate. Although a larger debate outside the scope of this paper exists regarding the extraterritorial application of human rights law, the underlying principles of both frameworks share a common theme—emphasizing independence and transparency in investigations. Despite the lack of clear requirements under international

¹¹ Michael W. Reisman, *The Lessons of Qana*, 22 YALE J. INT’L L. 381, 390 (1997).

humanitarian law, these principles provide a sufficient foundation upon which to evaluate existing investigatory mechanisms.

Part II examines the U.S. national investigatory process in detail, highlighting the major benefits and challenges of the system. Alternative investigation methods, including criminal law enforcement investigations, are considered before exploring in greater detail the primary mechanism currently used for civilian casualties in armed conflict—military command investigations. These military investigations benefit from not only significant resources and due process guarantees, but also a greater level of transparency due to the U.S. statutory right to request investigative reports after the fact. Nevertheless, the guidelines that allow investigating officers to be appointed from within the direct military chain of command contributes significantly to a perceived lack of independence. Two case studies—Haditha and Deh Rawood—demonstrate how these strengths and weaknesses affected the perception of the process and results of U.S. investigatory efforts. Without the ability for agencies outside the military chain of command, for instance representing the interests of civilian victims, to insert themselves into the vertical hierarchy of appointment and supervision of investigations, this perception will continue to fester.

Part III examines international investigatory processes created by both the human rights and IHL frameworks. A brief survey of human rights mechanisms reveals them less well-suited to the immediate needs of a timely civilian casualty investigation. A more detailed analysis of the IHFFC demonstrates that while it enjoys a strong perception of independence in the international community due to the composition of its investigating chamber, its limited resources and access threaten the accuracy of its investigative results. The effectiveness of the IHFFC is further impaired by limitations on its public transparency, which is dependent upon state consent. Ultimately, the inability of the United States to participate in investigations against its own troops, and conflicting national interpretations of obligations in war under international law, incentivizes the United States to not consent to the Commission's cognizance in most cases.

Part IV considers two alternatives to the current U.S. investigatory system, with an eye toward addressing the deficiencies identified by proponents of the IHFFC. The first alternative is the exclusive reliance on criminal law enforcement investigations, as embraced by British forces. The U.S. military criminal law enforcement system is subject only to the authority of the relevant Service Secretary, outside the influence of individual military units and most superior chains of command, allowing strict independence of the investigating officer up to the highest national levels. However, the privilege from disclosure granted to law enforcement sensitive material would result in a significant loss

of transparency in the process. The second alternative is the Joint Investigation Team, incorporating host nation officials into initial fact-finding operations in order to increase transparency to both the local populace and international community. Already commonly used in certain circumstances, this alternative directly addresses the problem of the vertical hierarchy identified in Part II.

Given the critiques identified in the previous sections, Part V recommends a way forward through changes to both systems. In order to increase the perceived independence of national investigating officers, the responsibility to appoint and supervise these officers should be transferred out (such as to the Inspector General's office), or up the chain of command to a higher authority sufficiently removed from the implicated unit, with the latter being more feasible due to institutional resource constraints. To increase transparency, unclassified summaries of investigation reports should be made publically available in a timely manner as standard practice. These changes would help satisfy two of the primary principles of both IHL and human rights law for proper investigations. The IHFFC remains a useful supplement to national investigations when the seniority of those implicated is such that no internal investigating officer could overcome a perceived lack of independence. In those limited circumstances, the U.S. could be convinced to consent to the Commission's cognizance if it guaranteed procedural safeguards more akin to national investigation procedures, drawing lessons learned from the investigation of Israeli action in the Gaza strip.

Although consenting to the IHFFC's cognizance would likely improve the international perception of U.S. accountability in civilian casualty incidents, little other incentive exists to consent. Because the Commission's strength lies primarily in the independence of its investigation body, consent would likely only be politically palatable in egregious cases implicating the upper echelons of U.S. political leadership. The interests of the local populace most directly affected by civilian casualty incidents are even less well served by the IHFFC procedure than national investigations. This paper argues that while the national investigatory system is far from perfect, consenting to the competence of the IHFFC in most cases will not significantly satisfy the underlying human rights principles it seeks to promote. Ultimately, for the majority of incidents, refining national procedures to better accord with underlying international principles would go farther to increase the accountability of the United States than turning to the IHFFC.

I. The Investigation Requirement

Human rights advocates have cited the United States' failure to admit wrongdoing on the part of its military, despite increasing civilian casualties, as a

failure to meet its obligations under both IHL and human rights law. IHL obligations are shaped by customary international law, the 1907 Hague Conventions,¹² and the Geneva Conventions of 1949 and subsequent Additional Protocols.¹³ The Geneva Conventions and subsequent Additional Protocols base state obligations in armed conflict on the principles of discrimination and proportionality. Discrimination requires that force be targeted against only military objects and objectives and not at civilian populations or objects (unless they are directly participating in hostilities).¹⁴ This principle is not necessarily breached if civilian casualties arise incident to an attack on a military objective. Proportionality requires that any expected incidental casualties not be excessive in relation to the anticipated concrete and direct military advantage to be gained by an attack on a military target.¹⁵ In general, these norms can be summarized to require that “no more force or greater violence should be used to carry out an operation than is absolutely necessary in the particular circumstances, if the

¹² Although used generically here, the term “1907 Hague Conventions” refers to multiple multilateral treaties signed at The Hague, Netherlands in the First Hague Conference of 1899 and the second Hague Conference of 1907. Four conventions were signed on July 29, 1899: Convention (I) Pacific Settlement of International Disputes; Convention (II) with Respect to the Laws and Customs of War on Land, 32 Stat. 1803; Convention (III) Adaptation to Maritime Warfare of Principles of Geneva Convention of 1864, 32 Stat. 1827; and Convention (IV) Prohibiting Launching of Projectiles and Explosives from Balloons, 32 Stat. 1839. 13 conventions were signed on October 18, 1907: Convention (I) for the Pacific Settlement of Disputes, 205 Consol. T.S. 233; Convention (II) for the Limitation of the Employment of Force for the Recovery of Contract Debts, 205 Consol. T.S. 250; Convention (III) Relating to Opening Hostilities, 205 Consol. T.S. 263; Convention (IV) Respecting the Laws and Customs of War on Land, 205 Consol. T.S. 277; Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 205 Consol. T.S. 299; Convention (VI) Relating to the Status of Enemy Merchant Ship, 205 Consol. T.S. 305; Convention (VII) Relating to the Conversion of Merchant Ships into Warships, 205 Consol. T.S. 319; Convention (VIII) Relative to the Laying of Automatic Submarine Contact Mines, 205 Consol. T.S. 331; Convention (IX) Concerning Bombardment by Naval Forces in Time of War, 205 Consol. T.S. 345; Convention (X) for the Adaptation of Principles of the Geneva Convention to Maritime Warfare, 205 Consol. T.S. 359; Convention (XI) Relative to Certain Restrictions with Regard to the Exercise of the Rights of Capture in Naval War, 205 Consol. T.S. 367; Convention (XII) for the establishment of an International Prize Court, 205 Consol. T.S. 381 [not ratified]; and Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, 205 Consol. T.S. 395.

¹³ The Geneva Conventions of 1949 include: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, August 12, 1949, 75 U.N.T.S. 31; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, August 12, 1949, 75 U.N.T.S. 85; Convention (III) relative to the Treatment of Prisoners of War, August 12, 1949, 75 U.N.T.S. 135; and Convention (IV) relative to the Protection of Civilian Persons in Time of War, August 12, 1949, 75 U.N.T.S. 287. The Additional Protocols, signed in 1977, include: Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I]; and Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609.

¹⁴ Protocol I, *supra* note 13, arts. 51-52.

¹⁵ *Id.*

application of such force would cause injury to non-combatants or civilians.”¹⁶ Military operations with significant civilian casualties that may rise to the level of war crimes are subject to additional IHL obligations to investigate and prosecute.

A. Under International Humanitarian Law

In his survey of legal requirements for such investigations, Michael Schmitt concludes that despite establishing the duty to investigate, neither existing customary international law nor the relevant IHL treaties provide sufficient practical guidance.¹⁷ The Geneva Conventions require state parties to “search” for and “prosecute” those accused of committing “grave breaches” of the Convention. Although no standards exist for the nature of the investigation, Schmitt deduces two general conclusions from the Geneva Conventions. First, the duty to investigate arises from an *allegation* of any conduct that may constitute a *war crime*. Second, an allegation must be *reasonably credible*, but may arise from *any source* and can be directed at *any level of responsibility* in the chain of command.¹⁸

Additional Protocol I also reference this duty, requiring military commanders and any member of the military to prevent, suppress, and report breaches of the Conventions to higher authorities.¹⁹ Although no detailed guidance is found in the Protocol or Commentary to it, Schmitt again draws a general conclusion that a state meets its obligations under the Protocol through the duty to report and investigate, which lies not only at the command level but also throughout the chain of command. Recognizing an “emphasis on the criticality of command as a mechanism for handling possible violations,”²⁰ investigations may be conducted by personnel within the same unit and should not undermine overall military effectiveness.

Finally, Schmitt refers to various interpretations of customary international law to support the general duty to investigate.²¹ Notably, the International Committee of the Red Cross has stated that “[s]tates must investigate war crimes allegedly committed by their national or armed forces,”²² while the U.N. General Assembly adopted guidelines stating that the obligation to respect IHL

¹⁶ LESLIE C. GREEN, *THE CONTEMPORARY LAW OF ARMED CONFLICT* 348 (2d ed. 2000).

¹⁷ Michael N. Schmitt, *Investigating Violations of International Law in Armed Conflict*, 2 HARV. NAT’L SEC. J. 31, (2011).

¹⁸ *Id.* at 36-39.

¹⁹ Protocol I, *supra* note 13, art. 87.

²⁰ Schmitt, *supra* note 17, at 43.

²¹ Schmitt, *supra* note 17, at 44-48.

²² INTERNATIONAL COMMITTEE OF THE RED CROSS, *CUSTOMARY INTERNATIONAL HUMANITARIAN LAW* (2005), Rule 158.

includes the duty to “[i]nvestigate violations effectively, promptly, thoroughly, and impartially.”²³ He suggests four “universal principles,” derived from the admittedly controversial 2009 Report of the United Nations Fact-Finding Mission on the Gaza Conflict [hereinafter the Goldstone Report]²⁴, to guide investigative efforts pursuant to IHL obligations: independence, effectiveness, promptness, and impartiality.²⁵

B. Under International Human Rights Law

In contrast to the vague investigatory requirements under IHL, human rights norms are significantly more detailed as a result of robust international and regional human rights jurisprudence. Despite their specificity, however, these norms remain highly debated in the United States and other countries due to required practices such as conducting autopsies, involving victims’ families, and maintaining chains of custody.²⁶ The European Court of Human Rights has interpreted the European Convention on Human Rights, which requires “an independent and impartial tribunal,” to prohibit participation by military officers on national security courts.²⁷ At the same time, rules governing trials for prisoners of war, which require “the essential guarantees of independence and impartiality as generally recognized,”²⁸ specifically allow military courts and authorities to conduct such trials.²⁹ This suggests that the parties to the Geneva Conventions did not consider military authorities to inherently lack independence and impartiality when evaluating military conduct, only that specific due process guarantees were required to ensure that independence and impartiality.

The United Kingdom addressed these due process guarantees directly in *Al-Skeini v. Secretary of State*,³⁰ while interpreting the right to life and prohibition from torture guaranteed in the European Convention for the Protection of

²³ *Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law*, G.A. Res. 60/147, Annex, U.N. Doc. A/RES/60/147, 3 (2005).

²⁴ U.N. Fact-Finding Mission on the Gaza Conflict, *Report of the U.N. Fact-Finding Mission on the Gaza Conflict*, U.N. Doc. A/HRC/12/48 (Sep. 25, 2009), <http://www2.ohchr.org/english/bodies/hrcouncil/docs/12session/A-HRC-12-48.pdf> [hereinafter Goldstone Report].

²⁵ *Human Rights in Palestine and other Occupied Arab Territories: Report of the United Nations Fact Finding Mission on the Gaza Conflict*, U.N. Doc. A/HRC/12/48, 1611 (2009).

²⁶ Schmitt, *supra* note 17, at 49 (citing McKerr v. United Kingdom, 111 Eur. Ct. H.R. 475 (2001)).

²⁷ *Incal v. Turkey*, IV Eur. Ct. H.R. 1547 (1998) (participation of military officials in court proceedings were “legitimate cause to doubt the independence and impartiality” of the court).

²⁸ Geneva Convention III, *supra* note 13, art. 84.

²⁹ *Id.* art. 87.

³⁰ *Al-Skeini v. Secretary of State for Defence*, [2004] EWHC 2911, [2004] All E.R. 197 (Q.B. Div’l Ct. 2004).

Human Rights and Fundamental Freedoms.³¹ The court held that the Convention implied a “procedural obligation of a proper and adequate investigation into loss of life,” without regard to the “difficulties created by situations of insurgency.”³² It declared ten requirements of investigations pursuant to the Convention:

1. An official investigation;
2. Open and objective oversight for the benefit of the deceased’s family and the public;
3. Explicit explanations when a person in custody dies;
4. Investigation even when state agency is not apparent;
5. Self-initiation by the state;
6. Capability to determine whether conduct was justified, and if not, identification and punishment of responsible parties;
7. Independence of the investigator from hierarchical and institutional connections to those implicated;
8. Sufficient public scrutiny;
9. Involvement of the next-of-kin; and
10. Proper, albeit not necessarily a single, procedure.³³

The court summarized its own universal principles, derived from its previous jurisprudence, to guide investigative efforts pursuant to human rights obligations: officialdom, timeliness, independence, openness, and effectiveness.³⁴

³¹ Sept. 3, 1953, 213 U.N.T.S. 222, *as amended* by Protocol 3, Sep. 21, 1970; Protocol 5, Dec. 20 1971; Protocol 8, Jan. 1, 1990; and Protocol 11, Nov. 1, 1998.

³² *Al-Skeini*, *supra* note 30, ¶¶ 319-20.

³³ *Id.* ¶ 321.

³⁴ *Id.* ¶ 322.

C. The Convergence of IHL and Human Rights Law

Some scholars argue that during times of armed conflict, human rights norms are superseded by IHL.³⁵ Some, like Schmitt, argue that investigatory standards created under human rights obligations in armed conflict can still be measured against IHL norms, pursuant to *lex specialis*.³⁶ Others insist on the full extraterritorial applicability of human rights norms in armed conflict.³⁷ While the debate continues,³⁸ it does not need to be resolved in order to determine the normative standard against which investigative requirements should be judged. In fact, although significant discussion surrounds the normative applicability of human rights law and institutions to armed conflict, less attention has been paid to the actual implementation measures. Naz Modirzadeh argues that this failure to critically consider specific implementation measures has in fact hurt the very civilian population that human rights advocates intend to protect.³⁹ The principle focus of applying human rights principles without heed to practical application detracts from the possibility of strengthening existing accountability mechanisms under IHL.⁴⁰ If human rights law advocates cannot translate accountability measures into terms that are acceptable to states, particularly military planners in states, they risk disregard and the perception of illegitimacy or irrelevance.⁴¹

Some military practitioners have agreed that the human rights framework, with some adjustment for the realities of military operations, is a valuable system of accountability. This is supposedly so given that specific standards for investigations are still developing under IHL framework.⁴² Kenneth Watkin notes that this “gap” in the level of accountability provided between the two frameworks is recognized in both public scrutiny and state reaction.⁴³ Addressing this “gap,” Françoise Hampson argued that “[t]he test for any

³⁵ See, e.g., Michael J. Dennis, *Non-Application of Civil and Political Rights Treaties Extraterritorially During Times of International Armed Conflict*, 40 ISR. L. REV. 453 (2007).

³⁶ Schmitt, *supra* note 17, 53-55, 82; cf. Noam Lubell, *Parallel Application of International Humanitarian Law and International Human Rights Law: An Examination of the Debate*, 40 ISR. L. REV. 648 (2007).

³⁷ Kenneth Watkin, *Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict*, 98 AM. J. INT’L L. 1 (2004).

³⁸ See, e.g., Naz K. Modirzadeh, *The Dark Sides of Convergence: A Pro-Civilian Critique of the Extraterritorial Application of Human Rights Law in Armed Conflict*, 86 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES (BLUE BOOK SERIES) 349, 350 and 401 n.4 (2010) (citing 40 ISR. L. REV. (2007); 90 INT’L REV. RED CROSS (2008)).

³⁹ Naz K. Modirzadeh, *The Dark Sides of Convergence: A Pro-Civilian Critique of the Extraterritorial Application of Human Rights Law in Armed Conflict*, 86 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES (BLUE BOOK SERIES) 349 (2010).

⁴⁰ *Id.* at 392.

⁴¹ *Id.* at 383-84.

⁴² Watkin, *supra* note 37, at 2.

⁴³ *Id.* at 24.

solution is that it must be both coherent and practical and should seek to avoid diminishing existing protection. It ought to be possible to achieve consensus on the implications in practice on the simultaneous applicability of IHL and human rights law.”⁴⁴

On a practical level, however, this gap is much smaller than the competing legal frameworks would suggest. Schmitt’s IHL principles for investigations are: independence, effectiveness, promptness, and impartiality. The U.K. court’s human rights principles for investigations are: officialdom, timeliness, independence, openness, and effectiveness. Adhering to the status quo that IHL norms govern investigation requirements, either as exclusive law or *lex specialis*, results in no different principles than under human rights law. The greater challenge in determining the proper method of investigation, therefore, is not in determining what normative standard to use, but in determining how to satisfy those underlying principles.

II. U.S. National Investigations

The current criticism of national investigatory processes reflects a lack of consensus on the “implications in practice” of such a system. U.S. national investigations are perceived as more biased, secretive, and focused on military strategy and preservation of the military force. The International Humanitarian Fact-Finding Commission is promoted as more independent, transparent, and focused on the rights of civilians. The procedural, legal, and political characteristics of both, however, demonstrate a strong degree of similarity in some key regards. Procedural characteristics of both include composition and expertise of the investigatory body, time requirements, resources, access to evidence (including *in situ* location, documents, and witnesses), actual reporting mechanisms, supervision over the investigation, external participation, due process guarantees, and public disclosure of findings. Legal characteristics include the mandate, scope of investigation, legal framework, standards of evidence, and legal effect. Political characteristics include intended audience, subsequent use, and impact on public opinion.

National investigations may take multiple forms, depending on the incident under review and the intended purpose of the report. Of primary importance is the sharp distinction made between criminal and administrative investigations. Criminal investigations within the military context are undertaken by professional law enforcement personnel, both military and civilian, when there is indication of criminal misconduct by a service member.

⁴⁴ Françoise J. Hampson, *The Relationship between International Humanitarian Law and Human Rights Law from the Perspective of a Human Rights Treaty Body*, 90 INT’L REV. RED CROSS 549 (2008).

Criminal law enforcement agencies—such as the Army Criminal Investigative Division (ACID) and the Naval Criminal Investigative Service (NCIS)—have primary investigative responsibility within their respective Service Departments for all major criminal offenses punishable under the Uniform Code of Military Justice (UCMJ) by confinement for more than one year.⁴⁵ They also have purview over any investigation into alleged violations of domestic federal criminal laws or foreign statutes when Department interests are involved.

Because the intended result is criminal prosecution or other disciplinary action, these investigations are characterized by their due process guarantees pursuant to the Uniform Code of Military Justice.⁴⁶ Before they are questioned, individuals suspected of criminal violations receive a rights advisement pursuant to Article 31(b) of the UCMJ—similar to *Miranda* warnings in civilian law enforcement—which includes a right to be informed of the nature of the charges and the right to remain silent. Searches and seizures are subject to probable cause requirements, similar to the standard warrant process. Evidence collection and retention procedures must maintain the chain of custody, sufficient for use at courts martial in accordance with the Military Rules of Evidence.

Conduct of criminal investigations is wholly within the discretion of the law enforcement agency head. The director of NCIS, for instance, reports directly to the Secretary of the Navy, and is authorized to initiate, conduct, and direct criminal investigations regardless of the authorization of the targeted subject's command.⁴⁷ Only the Secretary, with one exception for the Department of Defense Inspector General, may direct NCIS to delay, suspend or terminate an investigation.⁴⁸ Military commands are required to immediately refer to law enforcement agencies “any incidents of actual, suspected, or alleged major criminal offenses,” and provide subsequent logistical and personnel support while ensuring non-interference with investigative efforts.⁴⁹ Criminal law enforcement agencies may take cognizance of a case at any time, whether immediately upon notification of an incident or upon further development of facts from an administrative investigation. Therefore, criminal investigations

⁴⁵ See, e.g., U.S. DEP'T OF NAVY, SEC'Y OF NAVY INSTR. 5430.107, MISSION AND FUNCTIONS OF THE NAVAL CRIMINAL INVESTIGATIVE SERVICE ¶¶ 3.i, 4 (2005). [hereinafter SECNAVINST 5430.107] (defining major offenses and establishing primary jurisdiction for such cases pursuant to federal statute, Executive Order, and policy of the Departments of Defense and the Navy).

⁴⁶ DEPARTMENT OF THE NAVY, OFFICE OF THE JUDGE ADVOCATE GENERAL, MANUAL OF THE JUDGE ADVOCATE GENERAL, JAG Instruction 5800.7F (2012); § 0201(b) [hereinafter JAGMAN].

⁴⁷ SECNAVINST 5430.107, *supra* note 45, ¶ 6.a.

⁴⁸ *Id.* ¶ 7.c(1)(b).

⁴⁹ *Id.* ¶ 6.b(1)(a).

may be concurrent with, subsequent to, or in lieu of administrative investigations, but cannot be subsumed by the latter.⁵⁰

A. Administrative Investigations in General

By default, administrative investigations are reserved for incidents in which a command does not initially suspect a major criminal offense has occurred. Department of Defense administrative investigations, such as the after action report issued after NATO operations in Kosovo, are generally conducted on a national strategic level. Individual incidents are left to the cognizance of the responsible Service branch, which focuses on tactical and operational level concerns. U.S. domestic law authorizes each head of a Service branch to prescribe regulations for their own department.⁵¹ Generally, these service regulations⁵² grant fairly wide discretion to individual commanders to determine what type of administrative investigations may be appropriate and when they should commence.

Aside from specialized investigations, such as for counterintelligence efforts or medical quality assurance reviews, each Service generally recognizes at least five types of administrative investigations: preliminary inquiries, safety investigations, litigation reports, claims compensation investigations, and command investigations.⁵³

1. Preliminary Inquiries

Military regulations provide for the use of informal and prompt preliminary inquiries to determine the need and possible extent of further comprehensive investigation. Department of the Army regulations recommend preliminary inquiries in order to ascertain “the magnitude of the problem,”⁵⁴ as well as to determine whether a criminal, rather than an administrative investigation, is warranted. Department of the Navy (DON) regulations call for this process to be completed within three calendar days of learning of an incident, recognizing that extensions may be required for major incidents. Upon completion of the inquiry, a commander must report their decision whether or not to convene a subsequent command investigation to their immediate superior

⁵⁰ *Id.* ¶ 6b(6).

⁵¹ 5 U.S.C. § 301 (2015) (authorizes the head of a military department to prescribe government regulations of the department, “the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property” (subject to FOIA)).

⁵² *See, e.g.,* JAGMAN, *supra* note 46; DEPARTMENT OF THE ARMY, REG. 15-6, PROCEDURES FOR INVESTIGATING OFFICERS AND BOARDS OF OFFICERS (2 Oct. 2006) [hereinafter AR 15-6].

⁵³ JAGMAN, *supra* note 46, § 0201(c); AR 15-6, *supra* note 52, § 1-5.

⁵⁴ *Id.*

in the chain of command, who can concur with the recommendation or direct other action.⁵⁵ This reporting process is designed to ensure both timely notice of major incidents to higher authorities, as well as higher review of any determination that an incident does not warrant further investigation.

2. Litigation Reports and Claims Compensation

DON regulations distinguish incidents that are likely to result in claims or civil litigation brought in the United States against the Service, and imposes additional obligations on the investigating officer to gather facts and evidence in a manner protecting the legal interests of the government.⁵⁶ This primarily entails restricting access to investigation results to commanders and legal counsel representing the interests of the government. However, such reports are not to be used in the event of a “major incident,” which is defined as:

[a]n extraordinary incident occurring during the course of official duties resulting in multiple deaths, substantial property loss, or substantial harm to the environment, where the circumstances suggest a significant departure from the expected level of professionalism, leadership, judgment, communication, state of material readiness, or other relevant standard.⁵⁷

The major incident exception to litigation reports additionally defines substantial loss or harm as that “which greatly exceeds what is normally encountered in the course of day-to-day operations.” Incidents involving the death or substantial property damage of civilians during armed conflict would therefore be precluded from litigation report restrictions under this major incident exception.⁵⁸

Foreign claims compensation investigations for damages incident to noncombat military operations are the counterpoint to litigation reports. They are conducted in response to claims applications by civilians who have suffered the death of an immediate family member, injury, or property damages as a result of noncombat military activity or the negligent or wrongful acts or omissions of military personnel or employees outside of the United States.⁵⁹ The intent of the claims process is to accurately and expeditiously determine and pay

⁵⁵ JAGMAN, *supra* note 46, § 0204(b).

⁵⁶ *Id.* § 0210.

⁵⁷ *Id.* at append. A-2-a.

⁵⁸ *Id.* § 0209.

⁵⁹ JAGMAN, *supra* note 46, sec. 0812c; DEPARTMENT OF THE ARMY, REG. 27-20, CLAIMS para. 10-2 (8 Feb. 2008) [hereinafter AR 27-20].

out financial compensation for such death, injury, or damage.⁶⁰ Construing the legal authorities broadly, the United States “generally accepts responsibility for almost all” claims that result from the “negligent or wrongful act or omission” by U.S. personnel; claims-related investigations are, therefore, focused on whether U.S. personnel are responsible for the injury or damage and not on whether the level of culpability involved in the act or omission that resulted in the injury or damage.⁶¹

3. Safety Investigations

Under the cognizance of the Naval Safety Center, given the multi-billion dollar cost of damage to aircraft, ships, and other military vehicles, the primary intent of safety investigations is to derive lessons learned from mishaps in order to prevent such incidents from occurring again. Strict confidentiality and non-attribution of witness statements are therefore guaranteed in order to promote full disclosure of relevant circumstances without fear of criminal liability. Although statements made pursuant to a safety investigation may not be used for the purposes of any other administrative or criminal investigation, other investigations may be conducted concurrently using the same witnesses.⁶²

4. Command Investigations

Administrative investigations not otherwise regulated fall within the penumbra of what the services term “command investigations.” These are full investigations with the least restrictions on procedure and disclosure due to their general purpose nature. In such cases, the investigation of incidents is generally left to the discretion of the unit commander, subject to any preliminary inquiry requirements. The DON specifically recognizes that when an incident involves “large scale property damage, loss of life, or raises issues concerning the management of Naval activities, there may be sound policy reasons, such as openness and transparency of process or results, that warrant the convening of a command investigation.”⁶³ Additionally, it anticipates that administrative investigations may be appropriate for major incidents “accompanied by national public and press interest and significant congressional attention,” or having “the potential of undermining public confidence in the Naval service.”⁶⁴ Subsequent

⁶⁰ JAGMAN, *supra* note 46, sec. 0810c.

⁶¹ *Id.*

⁶² *Id.* at app. A-2-o.

⁶³ *Id.* § 0204(c)(1).

⁶⁴ *Id.* at app. A-2-a.

law enforcement investigations may result from possible criminal violations uncovered during the course of an administrative investigation.⁶⁵

B. The Policy of Civilian Casualties Investigations

Because civilian casualties during routine military operations in armed conflict are sometimes legally permissible under certain circumstances as collateral damage, they were traditionally not subject to full command investigations absent an indication of egregious behavior by military personnel. Egregious intentional killings were subject to criminal law enforcement investigations, while remaining damages were usually investigated only pursuant to limited claims investigations. For many years, the Department of Defense did not follow a department-wide policy requiring command investigations for civilian casualties. Each Service branch followed its own policy regarding such incidents, which usually relied ultimately on individual unit commander discretion. Only a commander concerned with policy reasons or public interest might have convened a command investigation for otherwise lawful casualties. As a result, no uniform tracking or investigation of civilian casualties existed during U.S. operations in Iraq, or during the early years of the conflict Afghanistan. No standard means existed to determine the circumstances of a civilian casualty incident, or even whether an investigation was convened.

In 2009, General Stanley McChrystal, Commander, International Security Assistance Force (ISAF) and Commander, U.S. Forces—Afghanistan (USFOR-A), changed this weak investigatory framework by issuing his revised Tactical Directive.⁶⁶ The Tactical Directive declared that military forces must “avoid the trap of winning tactical victories – but suffering strategic defeats—by causing civilian casualties or excessive damage and thus alienating the people.”⁶⁷ As part of this overall effort, ISAF and USFOR-A Civilian Casualty Tracking Cells were established a few months earlier in September 2008 in order to standardize tracking and investigating civilian casualty incidents in Afghanistan. Recognizing the difficulty posed by different national investigations, further regulations⁶⁸ mandated minimum standard requirements for coalition tracking. Because of General McChrystal’s dual role as commander of all U.S. and international troops in Afghanistan, the directive applied to all nations’ forces deployed for NATO operations, as well as U.S. forces deployed

⁶⁵ *Id.* § 0201(d).

⁶⁶ In 2006, then-Lieutenant General Peter Chiarelli, commander of Multi-National Corps – Iraq, directed an investigation be conducted in any case of death or serious injury to an Iraqi civilian. Thom Shanker, *New Guidelines Aim to Reduce Civilian Deaths in Iraq*, N.Y. TIMES, June 21, 2006, <http://www.nytimes.com/2006/06/21/world/middleeast/21cnd-casualties.html?pagewanted=print>.

⁶⁷ INTERNATIONAL SECURITY ASSISTANCE FORCE, HEADQUARTERS, TACTICAL DIRECTIVE (2009), available at <http://www.nato.int/isaf/docu/pressreleases/2009/07/pr090706-tactical-directive.html>.

⁶⁸ INTERNATIONAL SECURITY ASSISTANCE FORCE, STANDARD OPERATING PROCEDURES 302, 307.

under Operation Enduring Freedom. As a result, the disparate service approach in Afghanistan was altered to provide a unified baseline for more comprehensive national investigations of civilian casualties.

C. Command Investigations

The procedural aspects of a command investigation distinguish it from other investigatory processes—the appointment and supervision of the investigating body, resources and access to evidence and witnesses, due process guarantees, and publication of the report affect its legal and political impact. In general, command investigations emphasize efficiency, command responsibility, and individual rights. As a result, command investigations have limited legal authority and are primarily introspective. They are primarily to be used for internal lessons learned.

1. Appointment and Supervision of the Investigating Body

The conduct of military investigations is generally the responsibility of the unit involved in the incident, as carried out by an appointing authority and an investigating officer. Depending on the severity of the incident, either the unit commander or the first General or Flag officer⁶⁹ in the unit's chain of command will usually serve as the appointing authority, with occasional adjustments due to geographic restrictions. In major incidents, such as civilian deaths, DON regulations automatically elevate the appointing authority to flag level, regardless of unit responsiveness. This raises the level of visibility and accountability for major incidents to flag-level officers, who are held politically accountable to the Senate through their Advice and Consent power. The role of the appointing authority is three-fold: to appoint and resource the investigating officer, to define the scope of investigation, and to take action on the investigation's results.

The appointing authority (or “convening authority” in the Navy), with guidance from a cognizant legal advisor, may appoint anyone to be an investigating officer who is “best qualified for the duty by reason of their education, training, experience, length of service and temperament.”⁷⁰ Legal advisors, technical experts, interpreters, recorders, and other administrative support may be appointed to assist, but the investigating officer is solely

⁶⁹ 10 U.S.C. § 822 (2015). More specifically, this level is referred to as a General Court Martial Convening Authority, which includes the President, Secretary of Defense, relative service Secretaries, Unified and Combatant Commanders, and other flag officers as designated by the President or service Secretary.

⁷⁰ AR 15-6, *supra* note 52, § 2-1. JAGMAN, *supra* note 46, § 0206(b)(1) uses almost identical terms, but includes age of the investigating officer as a distinguishing factor.

responsible for the conduct, findings, opinions, and recommendations of the investigation report. The investigating officer may be a civilian employee, but in practice is generally a commissioned officer within the unit itself. The Navy explicitly recognizes that appointing an officer from a different unit may be more appropriate in certain situations, but treats such instances as the exception rather than the rule.⁷¹ The only enumerated requirement is that the officer be senior in rank to anyone whose conduct is under investigation, absent military exigencies, if adverse findings and recommendations are anticipated.⁷²

Impartiality is only explicitly recognized under the provisions for challenging the appointment of an investigating officer. Individuals designated as respondents in a formal board of inquiry have a recognized right to challenge an investigating officer.⁷³ This right does not, however, extend to investigations which do not result in a board of inquiry. Other interested parties may only present facts indicating a lack of impartiality or other qualification to the appointing authority.⁷⁴ An unfavorable decision by the appointing authority is final pursuant to Army Regulation 15-6 and the Judge Advocate General Manual (JAGMAN), and reviewable only under separate administrative complaint procedures.⁷⁵

Full administrative investigations are expected to be completed within 30 days, also allowing for exceptions for difficult major incidents.⁷⁶ Upon completion of the report, the appointing authority may approve, disapprove, modify, or add to findings of fact and opinions, comment on existing recommendations, state new recommendations as appropriate, indicate what corrective action is warranted or has been taken, and comment on the appropriateness of punitive or non-punitive action.⁷⁷

2. Resources and Access

Although the relationship between the appointing authority, investigating officer, and responsible unit raises questions about the impartiality of the investigation, it also provides for almost unlimited resources and access to relevant personnel and information. The appointment convening the investigation is a lawful military order, possessing the same legal effect as any other military order. Cooperation and support requested by the investigating

⁷¹ JAGMAN, *supra* note 46, § 0205.

⁷² AR 15-6, *supra* note 52, § 2-1; JAGMAN *supra* note 46, § 0206(b)(1).

⁷³ AR 15-6, *supra* note 52, § 5-7.

⁷⁴ *Id.* § 3-3.

⁷⁵ 10 U.S.C. § 938 (2015); U.S. DEP'T OF NAVY, U.S. NAVY REGULATIONS, 1990, art. 1150 (14 Sept. 1990).

⁷⁶ JAGMAN, *supra* note 46, § 0203(a).

⁷⁷ *Id.* § 0209(f).

officer is legally equivalent to any other military mission the unit is performing at the time, short of operational emergencies. Therefore, the entire financial and logistical weight of the DoD is available for conducting the investigation. This includes access to and maintenance of real evidence, including the chain of custody, which must be preserved by order of the investigating officer and documented in the report.⁷⁸ The investigating officer is tasked with ensuring evidence is safeguarded by the appropriate command.

Although the investigating officer does not have the authority to subpoena witnesses, appropriate commanders can order military and federal civilian employees to appear before the investigating body and issue invitational travel orders to other civilians if needed to facilitate the investigation.⁷⁹ The investigating officer may also order witnesses who are subject to military authority to refrain from discussing their testimony with other witnesses or interested parties in order to avoid undue influence until the investigation is complete. Witness statements, either taken verbatim or in narrative form, may be sworn and made under oath.⁸⁰ Portions of those statements are protected from disclosure under various guarantees, including the Privacy Act⁸¹ and the Health Insurance Portability and Accountability Act.⁸² Reflecting the heavy emphasis on distinguishing between safety, administrative, and criminal investigations, statements made for the purposes of a safety investigation may not be used in administrative investigations at all.

⁷⁸ AR 15-6, *supra* note 52, § 3-16; JAGMAN, *supra* note 46, § 0207.

⁷⁹ AR 15-6, *supra* note 52, § 3-8; JAGMAN, *supra* note 46, § 0207(d).

⁸⁰ AR 15-6, *supra* note 52, § 3-2.

⁸¹ 5 U.S.C. § 552a (2015).

⁸² 42 U.S.C. §§ 1320d to 1320d-9 (2015).

3. Due Process Guarantees

Army regulations do not distinguish due process guarantees between the investigation stage and subsequent accountability measures. The right to respond to information contained in a command investigation is aimed at protecting individuals from adverse action without procedural safeguards. Only those individuals who are named as respondents are guaranteed rights in the investigation process, which include the right to challenge board members and have legal counsel at a board of inquiry.⁸³ However, before the appointing authority may take final action against any individual based on the results of the investigation, that individual is guaranteed the right to review and respond to the evidence, findings, and recommendations made against them, including submission of rebuttal evidence.⁸⁴ Legal review is required for all cases involving serious matters such as death or serious bodily injury, to determine whether any substantial error occurred during the course of investigation that adversely affected an individual's substantial rights in a material way.⁸⁵ Adverse action is barred if it stems from any portion of the investigation that contained material errors.⁸⁶

Although DON regulations place greater distinction between the investigation and accountability phases, multiple due process guarantees exist even in the investigatory stage. For example, if the authority convening an investigation believes the interests of the individual whose conduct or performance of duty is called into question should be protected, a court or board of inquiry should be convened.⁸⁷ These inquiries are reserved for investigation of major incident, or serious or significant events, and utilize hearing procedures, legal counsel, advisors, and the power to compel testimony in the case of courts of inquiry, to assist in the fact finding process.⁸⁸ Moreover, if suspected of a criminal offense during the course of a command investigation, civilian employees are protected by any applicable collective bargaining requirements, while military personnel must be advised of their rights pursuant to Article 31 of the UCMJ.⁸⁹ Unless an investigation is deemed of no interest to anyone outside the command, an authority superior to that convening the investigation must review and endorse or modify it, and forward the

⁸³ AR 15-6, *supra* note 51, § 4-3.

⁸⁴ *Id.* § 1-9.

⁸⁵ *Id.* § 2-3.

⁸⁶ *Id.*

⁸⁷ JAGMAN, *supra* note 46, § 0204(c)(2).

⁸⁸ *Id.* § 0211

⁸⁹ *Id.* § 0207(c)(2).

investigation to all superior commanders who have a direct official interest in the incident.⁹⁰

4. Report Creation and Publication

Investigating officers are required to document their findings in a standard written report pursuant to the scope of the original appointing order, enclosing documentary evidence, witness statements, and photographs with the report, and noting the location of physical evidence. The report consists of the officer's findings of fact, opinions, and recommendations, based on their experience and subject matter familiarity. Factual findings may be based on any material the investigating officer deems relevant and material to an issue, with exceptions for certain privileged statements, supporting the occurrence of a particular fact as more likely than not.⁹¹ Although the investigator may draw reasonable inferences regarding what did or did not happen, mere speculating and theorizing into the motivation of individuals under investigation is prohibited.⁹² Any service member whom the investigating officer has made adverse recommendations against is entitled to the opportunity to review the evidence submitted against them and submit a written response. Ultimately, the investigating officer's recommendations must be based on the facts they determine to be true as well as an "understanding of the rules, regulations, policies, and customs of the service, guided by [the] concept of fairness both to the Government and to individuals."⁹³

Investigations are not considered final until reviewed and approved by the appointing authority.⁹⁴ Approval consists of ensuring the investigating officer has afforded this right of response, and that the report does not contain legal error or breaches of confidential information. Aside from the original terms of the convening order, at no time does the appointing authority shape the substance of the investigating officer's initial findings. The appointing authority is not permitted to change the stated findings of fact, opinions or recommendations of the investigating officer, but may disagree with the findings of fact or opinions or disapprove of the recommended action by supplemental memo.⁹⁵ The entire document is considered "For Official Use Only," and may

⁹⁰ *Id.* § 0209(g).

⁹¹ AR 15-6, *supra* note 52, §§ 3-7; 3-10.

⁹² JAGMAN, *supra* note 46, § 0207.

⁹³ AR 15-6, *supra* note 52, § 3-11.

⁹⁴ JAGMAN, *supra* note 46, § 0209(h).

⁹⁵ *Id.* § 209(f).

not be released outside routine business uses unless approved by the appointing authority or otherwise authorized by law or regulation.⁹⁶

Because routine business use anticipates wide circulation, classified information is expected to be omitted unless absolutely essential.⁹⁷ If not possible, investigating officers are encouraged to extract only unclassified information necessary from classified documents in order to write the report of investigation. Only if inclusion of classified information is unavoidable should a report be classified at the highest level pursuant to the highest level of classification of the evidence included in the report. It is possible, although rare, for the investigating officer or appointing authority to issue an unclassified summary of an otherwise classified report.⁹⁸

Investigations not restricted by security classifications are subject to public release pursuant to the Freedom of Information Act (FOIA).⁹⁹ FOIA enables anyone to request documents routinely maintained as a matter of record, subject to redaction of information in accordance with the Privacy Act, medical privacy laws, and routine FOIA exemptions.¹⁰⁰ These include redaction of classified information, internal personnel rules, information exempted by other statutes, interagency memoranda, and information being used for active law enforcement purposes. Exemptions are more likely to be prevalent in incidents which have not yet been resolved within the military chain of command, and less for incidents which have been resolved, regardless of actual disposition. Aside from these statutory restrictions, however, there are no limitations on who may make a FOIA request nor the type of investigation requested.

D. Critique of the Military Investigation System

Despite the procedural requirements laid out by military regulations, implementation of civilian casualty investigations in recent armed conflict has been inconsistent. These mixed results have spurred increasing criticism of the entire U.S. investigatory system, despite the fact that certain procedural guarantees, in fact, promote the same values espoused by critics. At the root of the debate is a tension between the transparency and independence of investigations and the military effectiveness of both the investigation procedure

⁹⁶ AR 15-6, *supra* note 52, § 3-18.

⁹⁷ JAGMAN, *supra* note 46, § 0208(b).

⁹⁸ See, e.g., UNITED STATES CENTRAL COMMAND, UNCLASSIFIED EXECUTIVE SUMMARY, INVESTIGATION OF CIVILIAN CASUALTIES, ORUZGAN PROVINCE, OPERATION FULL THROTTLE, June 30, 2002, *available at* <http://freerepublic.com/focus/f-news/972837/posts> [hereinafter CENTCOM].

⁹⁹ 5 U.S.C. § 552 (2015).

¹⁰⁰ JAGMAN, *supra* note 46, § 0209(h) (identifying legal authorities governing release of investigation reports outside the Department of the Navy).

as well as the underlying military operation. On the one hand, the lack of transparency in the wake of a major civilian casualty incident stokes suspicions of intentional targeting of civilians at worst, or negligent disregard of civilian lives at best. This phenomenon of “lawfare”¹⁰¹ can generate public backlash in response to suspicions of illegal conduct. American military efforts will remain vulnerable if the U.S. investigatory system does not address these concerns. On the other hand, total transparency could limit the effectiveness of military operations by exposing tactics, procedures, and practices that enemy forces could exploit if known. For instance, an innocent victim of an escalation of force incident may want to know what standoff distances were in place for engaging in lethal force. However, revelation of that information would only inform enemy forces of the maximum range they can approach U.S. forces before risking the use of lethal force against them.

Recognizing this tension, no reasonable critique of the U.S. investigatory system calls for transparency to the extent of full disclosure of confidential military operations. An appropriate standard balances these competing interests, ensuring an accurate account of factual circumstances and identifying where factual assessments may have been inaccurate, made independent of influence by the implicated unit. The lack of transparency, however, may be due to anything ranging from illegitimate intentional misrepresentation to legitimate constitutional protections. Currently, the U.S. investigatory system does not provide a means by which a critical public can evaluate the bases for the lack of transparency, whether an investigation was sufficiently independent, or a consistent means by which U.S. military or civilian leaders can explain why the lack of transparency is necessary. Two case studies¹⁰²—Haditha and Deh Rawood—illustrate how the U.S. investigatory system continues to suffer criticism with respect to these features, despite the extensive framework of openness and accessibility.

1. Case Study: Haditha

One of the most highly criticized civilian casualty incidents in the Iraq War fueled speculation of a system of intentional misrepresentation. The civilian casualties in Haditha became a public display of both the inherent weaknesses

¹⁰¹ For the initial introduction of the term, see Charles Dunlap, *Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts*, 20 (Carr Center for Human Rights Policy, Workshop Papers: “Humanitarian Challenges in Military Intervention” 2001).

¹⁰² In the author’s experience reviewing ISAF and U.S. civilian casualty investigations in Afghanistan, from 2009-2010, although these case studies involved dramatic civilian casualty incidents, the issues facing the investigators were not significantly different from incidents in which only one civilian was killed or injured. While the magnitude of reaction may not have reached the same level of international scrutiny, these smaller incidents nevertheless raised critiques similar to those made in the case studies.

and the possibilities of a U.S. investigatory system. The initial report, issued by the unit one day after the 19 November 2005 incident, stated that U.S. Marines had killed eight insurgents and wounded another in Haditha after suffering an attack by an improvised explosive device (IED), with one Marine and fifteen civilians dying as a result of the IED.¹⁰³ The media, however, received and aired a video showing numerous civilian casualties from that day, mostly composed of women and children.¹⁰⁴ Only after the media began questioning whether there had been a military cover-up did superiors in Iraq order a full preliminary inquiry on 14 February 2006.¹⁰⁵ That inquiry took almost a month to complete, at which point NCIS initiated a criminal investigation.¹⁰⁶ That was followed ser by the initiation of a full command investigation, to be conducted concurrent with the NCIS investigation by an Army major general.¹⁰⁷ Ultimately, only one Marine was convicted at court-martial as a result of the criminal investigation.¹⁰⁸ Superior officers were administratively punished for failing to investigate the matter initially,¹⁰⁹ although critics suggested that the subsequent investigation would never have occurred if the media had not aired and followed-up on the video footage.¹¹⁰

Haditha demonstrates the common environment surrounding command investigations that emphasize the primacy of military effectiveness over making accountability a priority. Command investigators in most civilian casualty incidents, not just Haditha, often go to great lengths to avoid accusing service members of improper conduct, let alone war crimes, in initial inquiries. This is due in large part to the desire to maintain military readiness. As one Army officer in Iraq stated, “You don’t want to create an environment where every time a soldier pulls the trigger, they think there’s going to be an

¹⁰³ Martin Asser, *What Happened at Haditha?*, BBC NEWS (Mar. 10, 2008, 5:12 PM GMT), http://news.bbc.co.uk/2/hi/middle_east/5033648.stm.

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ Josh White, *Report on Haditha Condemns Marines*, WASH. POST, Apr. 21, 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/20/AR2007042002308.html>.

¹⁰⁸ *Marine to Serve No Time in Iraqi Killings Case*, FOX NEWS, Jan. 24, 2012, <http://www.foxnews.com/us/2012/01/24/marine-to-serve-no-time-in-iraqi-killings-case/>; Tony Perry, *Marine Gets No Jail Time in Killing of 24 Iraqi Civilians*, L.A. TIMES, Jan. 25, 2012, <http://articles.latimes.com/2012/jan/25/local/la-me-haditha-20120125>.

¹⁰⁹ *Haditha Killings Fast Facts*, CNN (Mar. 14, 2015, 2:21 PM), <http://www.cnn.com/2013/10/30/world/meast/haditha-killings-fast-facts/>.

¹¹⁰ See Sidney Blumenthal, *George Bush Sr. Asked Retired General to Replace Rumsfeld*, SALON (June 8, 2006, 9:00 AM), http://www.salon.com/2006/06/08/haditha_4/; Tony Perry & Julian E. Barnes, *Photos Indicate Civilians Slain Execution-Style*, L.A. TIMES, May 27, 2006, <http://articles.latimes.com/2006/may/27/world/fg-marines27>.

investigation.”¹¹¹ Therefore, a command’s initial tendency is to classify an incident, if at all possible, as the normal conduct of war. In the case of Haditha, this meant initially classifying those killed either as combatants, individuals displaying hostile intent, or collateral damage in pursuit of legitimate military targets.

In Michael Walzer’s critique of the military justice system, he notes that this tendency is due to the fact that the same hierarchical chain of command that is responsible for ordering and carrying out the mission is also responsible for evaluating its legality.¹¹² The rights and interests of civilians lay outside that chain, with no advocate able to penetrate it from the outside. In the case of Haditha, it was not until media reports exposed the number of clearly identifiable women and children among the dead that superiors in the chain of command ordered further investigation. The involvement of external parties, however, is neither invited nor necessarily possible, as in the case of unsecure locations or populations which journalists and non-governmental organizations (NGOs) are not able to access. Without some way of guaranteeing this insertion into the chain of command, the perception of national bias or a cover-up will remain.

Once the U.S. investigation was initiated in Haditha, it proceeded as designed but still was subject to significant pressure from both military and civilian leaders. The NCIS investigation focused on criminal liability of individual unit members, while the command investigation emphasized deficiencies in training, resourcing, rules of engagement, leadership, and command responsibility. The command investigation’s intent was not to prosecute individuals for war crimes, but to examine the operational environment in order to identify lessons that could be learned and avoid similar incidents in the future. Whether the initial report of insurgent deaths was the result of intentional misrepresentation or a reluctance to second-guess service members on the ground, the public perception of a military cover-up influenced the perceived legitimacy of the results of the subsequent investigation.

2. Case Study: Deh Rawood

The pressure to maintaining military efficacy was also evident years earlier in Afghanistan. On the night of June 30, 2002, 48 people—mostly women and children—were killed in an air strike in Kakarak, in the Deh Rawood area of Uruzgan province. The mission was to destroy an identified

¹¹¹ See Jacki Lyden & John McChesney, *Anatomy of a Shooting: A Civilian’s Death in Iraq*, ALL THINGS CONSIDERED (June 23, 2006, 11:37 AM), <<http://www.npr.org/templates/story/story.php?storyId=5506353>.

¹¹² MICHAEL WALZER, ARGUING ABOUT WAR 23-32 (2004).

enemy stronghold in Deh Rawood while in search of a high value Al-Qaeda leader believed to be in the area. According to initial U.S. accounts, aircraft dropped munitions on a compound in response to what it believed to be anti-aircraft fire. Locals disputed the claim, saying it was celebratory small arms fire emitting from a wedding-engagement party, which is common in Afghanistan.

Three separate national and coalition investigations were launched within days of the incident. Coalition ground forces attempted to conduct a Battle Damage Assessment immediately; a U.S. and Afghan joint task force initiated a preliminary inquiry approximately three days after the incident; and a formal command investigation commenced approximately 30 days later. In what some have lauded as an extraordinary step toward greater transparency, the military released an unclassified version of the investigation.¹¹³ It found no fault on the part of U.S. and coalition forces—maintaining the aircraft was subjected to sustained direct fire—but it did expose the justifications relied upon by U.S. and coalition forces to attack the compound. Although senior leaders initially denied any mistake or wrongdoing,¹¹⁴ they reportedly acknowledged to Afghan leaders unofficially that the ground and aircrews made a mistake.¹¹⁵ This admission, combined with monetary pledges to rebuild infrastructure in the region, reportedly helped ease tensions with the local Afghan population.¹¹⁶

U.S. officials nevertheless had to defend against accusations of a cover-up. A preliminary U.N. fact-finding report, leaked to the press before it was finalized, supposedly accused U.S. forces of removing evidence from the scene and cited higher civilian casualty numbers than eventually reported. In the wake of press reports, the U.N. quickly withdrew the accusation as without basis.¹¹⁷ The transparency of the Deh Rawood investigation goes to the foundation of the U.N. Special Rapporteur's critique of the national investigatory process. He advocated for greater respect for the principles of accountability and transparency, so that any individual affected by such incidents can personally appeal to the local military unit and receive honest answers about the fate of loved ones. The immediate response to investigate the incident, subsequent interaction with the Deh Rawood residents, and final publication of an

¹¹³ See CENTCOM, *supra* note 98.

¹¹⁴ See, e.g., Luke Harding, *No US Apology Over Wedding Bomb*, THE GUARDIAN, July 3, 2002, <http://www.guardian.co.uk/world/2002/jul/03/afghanistan.lukeharding>.

¹¹⁵ See, e.g., Michael Ware, *Afghan Says U.S. to Help Wedding Victims*, TIME, July 10, 2002, <http://www.time.com/time/world/article/0,8599,319710,00.html>.

¹¹⁶ See, e.g., Alissa J. Rubin, *U.S. Raid on Village Prompts Afghans to Demand Changes in War Strategies*, LOS ANGELES TIMES, July 15, 2002, <http://articles.latimes.com/2002/jul/15/world/fg-raid15>.

¹¹⁷ U.N. *Revises Afghan Wedding Attack Report*, CNN, July 29, 2002, http://articles.cnn.com/2002-07-29/world/un.afghan.wedding_1_fact-finding-team-fact-finding-mission-afghanistan?_s=PM:asiapcf.

unclassified summary all attempted to address concerns about the transparency of the process. Despite the investigation's ultimate conclusion that no liability should attach to the air or ground crew, the process of the investigation itself was validated while the U.S. was still able to maintain control over the investigation and military effectiveness. Contrast this to the Haditha investigation, which resulted in limited criminal and administrative punishment, but was wrought with accusations of a cover-up. The result of the investigation itself became secondary to the transparency of the process. So long as the process relies solely on the vertical hierarchy between the appointing authority and the unit involved, civilian interests will not be perceived as being adequately addressed.

III. International Investigations

Given the obstacles to transparency inherent in the U.S. investigatory system, international mechanisms offer a potential solution. As previously discussed, successful investigatory standards are not inherently rooted in one particular legal framework—both international human rights law and IHL support similar principles. Given the convergence of principles, it is worthwhile to consider how investigatory mechanisms within each system function, and whether they would be appropriate in the context of investigating civilian casualties in armed conflict.

A. The Human Rights Approach

Prior to World War II, investigation into violations of international humanitarian law was primarily the sovereign responsibility of individual nations. Even after the Nuremberg trials, it took years before states routinely began to call for *de novo* international review of national conduct. Although intergovernmental and NGOs like the International Committee of the Red Cross (ICRC) and Human Rights Watch have traditionally monitored violations of international law, the idea that the international community would undertake to compile a version of events independent of a national investigation was “virtually unthinkable,” until only recently.¹¹⁸ The ICRC noted that the increase in investigations by U.N. agencies—such as the U.N. Commission on Human Rights and the Inter-American Commission on Human Rights—is due in part to “the lack of mandate among IHL mechanisms to deal with non-international armed conflicts.”¹¹⁹ Challenged by the inability to enforce accountability of non-

¹¹⁸ HENRY J. STEINER ET AL., INTERNATIONAL HUMAN RIGHTS IN CONTEXT 747 (3d ed. 2007).

¹¹⁹ INTERNATIONAL COMMITTEE OF THE RED CROSS, IMPROVING COMPLIANCE WITH INTERNATIONAL HUMANITARIAN LAW 8 (2004).

state actors,¹²⁰ however, such agencies remain best-suited to address conduct by states which are parties to various U.N. conventions and treaties. Within this environment, human rights advocates assess the credibility and potential impact of an investigation by “the extent to which it is perceived to have been thorough, politically objective, and procedurally fair.”¹²¹

Despite the growing consensus that international investigation is necessary, however, there is a lack of consensus within the international human rights community regarding what constitutes a “thorough,” “objective,” or “procedurally fair” investigation. The community remains critical of the independence and transparency of the U.S. national investigative process, in spite of its detailed procedural guidelines and extensive available resources. However, rather than adopt a standardized approach, advocates have relied on individual precedents of successful investigations to guide a generalized, situation-dependent process. An early precedent was the 1978 Memorandum of Understanding negotiated by the UNCHR ad hoc Working Group with the government of Chile.¹²² This became a *de facto* template for subsequent fact finding missions, and was incorporated three years later into the International Law Association’s “The Belgrade Minimum Rules of Procedure for International Human Rights Fact-Finding Missions.”¹²³

Fact finding by international human rights treaty bodies usually entails one of three major procedures – examinations of state reports, inquiries based on individual complaints, or country/thematic investigations.¹²⁴ U.N. treaty bodies, such as the Human Rights Committee and Committee Against Torture, and regional bodies, such as the Inter-American Commission on Human Rights, examine both state reports as well as inquiries by individual communications. The U.N. Human Rights Council appoints rapporteurs under their special procedures to investigate a specific country or thematic violation. Between these procedures, there is no standard for the length of evaluation, locality of investigation, required specificity of complaints, theme, information gathering process, or adjudicative functions.¹²⁵

¹²⁰ *Id.* at 9 (these agencies attempt to address the conduct of non-state actors “in reports or General Recommendations, or by finding States responsible for omission or acquiescence in the face of violations by armed groups”).

¹²¹ STEINER ET AL., *supra* note 118, at 747.

¹²² UN Doc. A/33/331, Annex VII (1978).

¹²³ See STEINER ET AL., *supra* note 118, at 750.

¹²⁴ Frans Viljoen, *Fact-Finding by UN Human Rights Complaints Bodies—Analysis and Suggested Reforms*, 8 MAX PLANCK Y.B. OF UNITED NATIONS LAW 49, 54 (2004).

¹²⁵ DAVID WEISSBRODT ET AL., INTERNATIONAL HUMAN RIGHTS: LAW, POLICY AND PROCESS 588 (4th ed. 2009).

1. Examination of State Reports

This form of “indirect fact-finding” is used to assess compliance with party treaty obligations, as evidenced through state submission of initial and periodic written reports.¹²⁶ A significant portion of this process depends on a dialogue between the fact-finding body and government under investigation, as well as the fact finding body’s concluding observations.¹²⁷ Other interested parties, such as NGOs, are permitted to submit companion reports to supplement or counter factual assertions made in the government reports. Because examination is limited to written testimony, however, assessing factual accuracy is often hampered by government denial of allegations without supporting evidence or counterfactuals.¹²⁸ Moreover, if the state reporting system were extended to IHL obligations, critics have noted:

Any compliance control system in international humanitarian law affects a state’s sovereignty in its essence and therefore states’ willingness to adhere to a strict system of substantive obligations is considerably low [A member state] would be most reluctant to reveal its practices concerning means and methods of warfare and to participate in a reporting system comprising of the substantive humanitarian law obligations.¹²⁹

The lengthy response times and reliance on government testimony to self-report treaty violations make examination of state reports more appropriate for ensuring broad human rights treaty compliance, rather than investigation into specific incidents of civilian casualties during armed conflict.

2. Individual Complaints

Four of seven current human rights treaties provide mechanisms to evaluate individual rights of action against state party violation of its obligations.¹³⁰ An individual is required to first exhaust all local remedies within the state of complaint, or else allege the state system is unable to provide effective remedy. The complaint bodies, composed of members elected from the treaty parties representing an equitable geographical distribution, usually defer

¹²⁶ Viljoen, *supra* note 124, at 59 (citing F. Ermacora, *International Enquiry Commissions in the Field of Human Rights*, 1 REVUE DE DROITS DE L’HOMME/HUM. RTS. J. 180, 186 (1968)).

¹²⁷ Viljoen, *supra* note 124, at 60.

¹²⁸ *Id.* at 59.

¹²⁹ Heike Spieker, *The Possible Shape of a Reporting System for IHL*, in TOWARDS A BETTER IMPLEMENTATION OF INTERNATIONAL HUMANITARIAN LAW 83, 87 (Michael Bothe ed., 2001).

¹³⁰ These are the Committee on the Elimination of Racial Discrimination, the Human Rights Committee, the Committee Against Torture, and the Committee on the Elimination of Discrimination against Women (which transferred its functions to OCHCR in 2008).

to domestic judgments on factual matters, absent evidence of manifest arbitrariness or injustice.¹³¹ If a written complaint against a state is certified as admissible by the treaty body, a response is requested from the accused state, with the individual complainant given a right of response. Unlike the state report examination process, third parties to the process usually may not submit evidence. The exception is the Working Group on Arbitrary Detention, which draws its mandate from Article 56 of UN Charter.¹³² The working group may conduct *in loco* country visits and, unlike other complaint bodies, may draw on evidential reports submitted by third parties (including other U.N. special mechanisms and treaty bodies). Although the remaining complaint bodies are not prohibited by treaty from conducting oral hearings or investigations, the lack of resources to fund travel and dependence on state consent limit the effectiveness of these bodies when they do convene an investigation.¹³³

The remaining complaint bodies are also challenged by the common state practice of blanket denial of allegations without providing a counterfactual. They must create a factual narrative and attempt to form conclusions based solely on the complainant's allegations.¹³⁴ In certain human rights contexts, such as cases of non-refoulement, the complaint body will favor the state in the absence of reliable contradictory evidence. In others, it will proceed with the allegations if the state fails to respond substantively. This process has been criticized for its time-consuming written format and inconsistent approach to conducting *de novo* fact-finding investigations, which leads to a perception that "the unavailability of relevant information may have resulted in decisions which were, either in law or in fact, incomplete or misleading."¹³⁵ The nature of these complaints bodies has been criticized for its inability to adequately monitor remedial action.¹³⁶ Because the conclusions are mere opinions, per the U.N. treaty mandate, they carry no legal effect and rely on the larger political body to enforce its findings.¹³⁷ For example, although the Human Rights Committee provides states 90 days to begin responding to individual allegations, the

¹³¹ Viljoen, *supra* note 124, at 70-86 (CAT Committee General Comment No. 1, para. 9, contained in U.N. Doc. A/53/44, Annex IX of 21 November 1997; principle of geographic representation embodied in ICCPR Arts 29(3) and 31(2); Optional Protocol to CAT subcommittee guided by principles of confidentiality, impartiality, non-selectivity, universality and objectivity, containing in U.N. Doc. A/RES/57/199 of Dec. 18, 2002, para. 2(3)).

¹³² See Hum. Rts. Comm., 49th Sess., U.N. Doc. E/CN.4/1993/24.

¹³³ Douglass W. Cassel, *Fact-Finding in the Inter-American System*, in THE UN HUMAN RIGHTS TREATY SYSTEM IN THE 21ST CENTURY 105, 107 (Anne F. Bayefsky ed., 2000).

¹³⁴ Viljoen, *supra* note 124, at 71.

¹³⁵ Viljoen, *supra* note 124, at 84 (citing Markus Schimdt, *Individual human rights complaints procedures based on United Nations treaties and the need for reform*, 41 INT'L & COMP. L.Q. 645, 652 (1992)) (arguing for oral hearing to address concerns, referring to *Lubicon Lake Band* case in which initial complaint was submitted 1984 but final decision not reached until 1990).

¹³⁶ Viljoen, *supra* note 124, at 75.

¹³⁷ *Id.* at 63.

committee must rely on state reporting or NGO monitoring to ensure effective compliance.

Although the individual complaints process is better suited than state reports to investigate individual incidents as they arise, the cumbersome written exchanges and lack of mandate for *de novo* fact finding can limit the accuracy and effectiveness of any factual accounting.

3. Country/Thematic Investigations

U.N. special procedures are designed to investigate the conduct of a single country with regard to multiple international norms, or global conduct with regard to a single international norm. Investigations may be requested by the various U.N. bodies, including the U.N. Commission on Human Rights, or other human rights advocates. The piecemeal development of the special procedures process by different interest constituencies, however, has resulted in a lack of standard procedures or format for these investigations. Even the basic premise that investigations can provide “the establishment of truth” has been questioned as “inherently subjective”—dependent on so many contextual factors that “[i]t is impossible to find the ‘real facts’ or truth,” both as a matter of epistemology and pragmatism.”¹³⁸ Standardized terms of reference for UN Special Rapporteurs were not established until almost 20 years after the International Law Association approved the Belgrade Minimum Rules of Procedure in 1980.¹³⁹ When finally enumerated, these included requesting guarantees from the host government for security, freedom of movement, and freedom of inquiry. Freedom of inquiry was defined by access to locations, documents, government officials, and confidential and unsupervised witness visits free from retribution.

Even with the development of more standardized terms of reference, investigations by various treaty bodies remain the exception.¹⁴⁰ For example, the Human Rights Committee of the International Covenant on Civil and Political Rights emphasizes the importance of fair procedures through *audiatur et altera pars*, to ensure its written reports provide an unbiased and substantiated platform for political discussion. Recognizing that inaccuracies may result due to the variety of evidentiary sources, including written government reports, the

¹³⁸ *Id.* at 52 (citing Kurt Herndl, *Recent Developments Concerning United Nations Fact-Finding in the Field of Human Rights*, in *PROGRESS IN THE SPIRIT OF HUMAN RIGHTS* 32 (M. Nowak et al. eds., 1988)).

¹³⁹ TERMS OF REFERENCE FOR FACT-FINDING MISSIONS BY SPECIAL RAPORTEURS/REPRESENTATIVES OF THE COMMISSION ON HUMAN RIGHTS, UN Doc. E/CN.4/1998/45, app. V.

¹⁴⁰ Viljoen, *supra* note 124, at 56.

Committee Against Torture allows on-site inquiries and supplementary preventive visits. The optional protocol to the Committee to End Discrimination Against Women (CEDAW) allows confidential inquiries when the Committee is informed of violations, provided the offending state consents. In addition to relying on written information presented by the government, CEDAW can meet with government delegations in the U.N. or during country visits to supplement its fact-finding process.

B. An International Humanitarian Law Approach

U.N. investigations can be distinguished between those focused on sustained human rights violations within or among states, as discussed above, and those focused on discrete violations of international humanitarian law. Article 90 of Additional Protocol I of the Geneva Convention of 1949 provides for the creation of an International Humanitarian Fact-Finding Commission for such violations. Although the Commission has yet to be called upon since its establishment in 1991 by a state party to investigate a major civilian casualty incident, many NGOs and human rights advocates continue to call for its employment. In 1992, the Commission adopted rules for the conduct of fact-finding inquiries, and these rules were amended in 1993. Although the specific provisions are relatively less detailed than U.S. investigation procedures, they are sufficient to highlight the distinction between the two processes.

1. Competence of the Commission

The Commission is mandated to inquire into any facts alleged to be a “serious violation” or “grave breach” (as defined in the Conventions and Additional Protocols), and “facilitate . . . the restoration of an attitude of respect for the Conventions.”¹⁴¹ Commission investigations can only be initiated by state parties to a conflict, who are either signatories of the Geneva Conventions or consent to the Commission’s competence. The Commission cannot act on its own initiative, or on the basis of allegations by individuals or third-party organizations, without the consent of the parties to the conflict. A review of the treaty text and deliberations by the contracting parties reveals that competency was specifically restricted to international armed conflict in order to prevent interference with a state’s internal affairs.¹⁴² Although some scholars have

¹⁴¹ Protocol I, *supra* note 13, art. 90 § 2(c); *see also* RULES OF THE INTERNATIONAL HUMANITARIAN FACT-FINDING COMMISSION, § 28-1 (adopted 8 July 1992, amended 11 Mar. 2003, 13 Feb. 2009, 11 Feb. 2011, and 26 Mar. 2014) [hereinafter IHFFC RULES], available at http://www.ihffc.org/index.asp?Language=EN&page=rules_of_commission.

¹⁴² August Reinisch, *The International Fact-Finding Commission According to Art. 90 Additional Protocol I to the Geneva Conventions and its Potential Enquiry Competence in the Yugoslav Conflict*, 65 NORDIC J. INT’L L. 241, 246 (1996).

suggested that a liberal reading of “serious violations” pursuant to Common Article 3 would extend the Commission’s competence to non-international armed conflict, this remains the subject of debate.¹⁴³ However, not only has the Commission declared its willingness to investigate incidents of non-international armed conflict if all parties to the conflict consent, it has suggested that parties “might properly be strongly urged to give consent” or be required to be subject to an inquiry undertaken under the Chapter VII powers of the UN Security Council.¹⁴⁴

2. Appointment of Investigating body, Timeline, and Supervision

The Commission itself is composed of fifteen members, nominated from and elected every five years by the High Contracting Parties to Additional Protocol I. Current commission members include experts in medicine, the judiciary, military, public diplomacy, and international law.¹⁴⁵ Elected members serve in their personal capacity, not as agents of their respective governments, and are specifically prohibited from accepting “instructions from any authority or person whatsoever.”¹⁴⁶ Expected to possess “high moral standing and acknowledged impartiality,”¹⁴⁷ members are entreated to refrain from making public statements or undertaking occupations during their term which would cast doubt on their morality or impartiality.¹⁴⁸ The position is unpaid to ensure independence from national or other external influences. But despite this stated commitment to national impartiality, Article 90 nevertheless requires equitable geographic representation in overall Commission membership.¹⁴⁹ One the one hand, this may encourage procedural neutrality in an otherwise contentious process, but on the other, this suggests an underlying suspicion of inherent national bias. It also leaves almost no room for states to challenge a Commission member’s appointment for other reasons.

¹⁴³ *Id.* at 251 (“a State making allegations may also bring a request for enquiry—a result which is also more in conformity with political reality and the likelihood of activating the Commission’s enquiry capacity, since it will be most probably a State considering itself aggrieved by violations of humanitarian law who will demand an enquiry of its allegations”).

¹⁴⁴ *Annual Report 2009*, INTERNATIONAL HUMANITARIAN FACT-FINDING COMMISSION, http://www.ihffc.org/Files/fr/pdf/ihffc_annual_report_2009.pdf.

¹⁴⁵ *Id.*

¹⁴⁶ IHFFC RULES, *supra* note 141, §1-1.

¹⁴⁷ Protocol I, *supra* note 13, art. 90 § 1(a).

¹⁴⁸ IHFFC RULES, *supra* note 141, § 3.

¹⁴⁹ The current composition of members includes individuals from Japan, Germany, Switzerland, Chile, United Arab Emirates, Uruguay, Algeria, Poland, Lithuania, Argentina, United Kingdom, Italy, Greece, Belgium, and Russian Federation. *Members of the IHFFC*, INTERNATIONAL HUMANITARIAN FACT-FINDING COMMISSION, <http://www.ihffc.org/index.asp?page=members> (last visited June 8, 2015).

The appointment of the actual investigatory body likewise emphasizes geographic considerations. Investigations are conducted by a Chamber comprised of seven Commission members. The Commission President appoints five members to the Chamber on the basis of geographic distribution, while the remaining two members are chosen by each side to a conflict as “ad hoc” Chamber members. The only restriction is that no Chamber member may be a national of any party to the conflict under investigation. No additional qualifications are required for Chamber appointment. Members may, however, recuse themselves from an investigation if they deem appropriate.¹⁵⁰

Because Article 90 does not enumerate a time line, no standard exists by which to enforce or evaluate the timeliness of the Commission’s response to allegations. Instead, the Commission President is responsible for establishing an appropriate time limit for establishing the Chamber. If members are not appointed within the determined amount of time, the President may make immediate appointments as necessary.¹⁵¹ After the Chamber has been established, the President’s responsibility during the fact finding process is complete, except for ensuring that administrative support is available. Similar to the relationship between the investigating officer and appointing authority in U.S. investigations, while the Chamber is completely autonomous during its fact-finding process, the Commission as a whole issues the final report of findings and recommendations, as appropriate.¹⁵²

3. Resources and Access

Although Article 90 establishes the authority of the Commission, it does not provide for independent funding or resources. As such, the Commission’s functioning is highly dependent on extensive support and participation by the High Contracting Parties. Administrative facilities are provided by the Swiss Depositary, and administrative expenses are met by the High Contracting Parties. The Commission may authorize administrative and technical support to the Chamber, including subject-matter experts and interpreters, for an investigation¹⁵³ who are bound by the same confidentiality pledge as members.¹⁵⁴ The Commission eventually adopted a financial structure reflecting responsibility for expenses proportionate to U.N. General Assembly distributions. Any funding required in advance of an investigation is provided by the party to the conflict requesting the investigation. That state is entitled to

¹⁵⁰ IHFFC RULES, *supra* note 141, § 23.

¹⁵¹ *Id.* § 23(c).

¹⁵² *Id.* § 28.

¹⁵³ *Id.* § 25.

¹⁵⁴ *Id.* § 29.

reimbursement by the party against which allegations are made—up to half the costs to the Chamber.

The Commission relies on evidence presented by states, as well as third-party evidence, and evidence gathered independently *in loco*.¹⁵⁵ Access to witnesses, documents, and locations is primarily dependent on state cooperation, since the Commission possesses no inherent authority to demand access or ensure preservation of evidence. Similar to the special procedures standards, the investigatory body is dependent on the host government assuring access to witness interviews and documentary evidence. The Head of the Chamber is responsible for registration and custody of all evidence, which is transferred to the custody of the Secretariat upon completion of the investigation.¹⁵⁶ Individual chamber members may attempt, however, to conduct an *in loco* inquiry immediately after an allegation is made in order to preserve evidence, pursuant to the 1946 Convention on Privileges and Immunities of the United Nations.¹⁵⁷

4. Due Process Guarantees

Because the focus of Commission investigations is on state conduct, the rights of individuals involved in an incident are of less concern than the rights of the state as a singular entity. The process emphasizes ensuring a broad factual basis upon which the Chamber can make a determination. Therefore, the Chamber will hear from any person who might assist in an investigation.¹⁵⁸ The two primary due process guarantees are a state's right to challenge both the Commission's competence as well as any evidence submitted against it.

Before the Chamber can commence an investigation, it must ensure that all states have consented to its competence.¹⁵⁹ The prohibition against third-party initiated inquiries prevents secret allegations or investigations to which a state does not consent. The requesting state must allege a grave breach or serious violation with specificity, including evidence in support of its claim. If the target state contests the grounds as outside the Commission's competence, the dispute is to be resolved through "speedy consultation" with an undefined arbiter. If the Commission pursues the investigation, all evidence must be fully disclosed to the state under investigation. That state has the right to present evidence in its defense and comment on the allegations, within a fixed period of time.¹⁶⁰

¹⁵⁵ Protocol I, *supra* note 13, art. 90 § 4(a).

¹⁵⁶ IHFFC RULES, *supra* note 141, § 24.

¹⁵⁷ *Id.* § 27.

¹⁵⁸ *Id.* § 19.

¹⁵⁹ *Id.* § 20.

¹⁶⁰ *Id.* §§ 21, 27, 28.

Similar to U.S. investigations, if a state fails to provide evidence to counter an allegation, the Commission report is expected to make note of the deficiency, rather than infer conclusions with no evidentiary basis. Unlike U.S. investigations, however, no final review exists to determine whether the state's rights have been preserved, or whether the investigation contains material errors.

5. Report and Publication

Upon completion of its investigation, the Chamber reports its findings of fact and recommendations to the entire Commission. The Commission decides by majority if a consensus cannot be reached, but considers the Chamber's findings rejected if a majority is not obtained.¹⁶¹ If insufficient evidence exists to evaluate the allegation, the Chamber is expected to document the reasons for its inability to secure sufficient evidence. Copies of the report and recommendations are sent to the state parties to the conflict and are accessible to the Commission members themselves only while they are in office.¹⁶² Neither the results of the investigation nor any personal data of individuals involved may be published without the express consent of the states and persons concerned.¹⁶³ Members and assistants are sworn to maintain confidentiality with regard to any facts or information disclosed in the course of the investigation.

C. Critique of the International Humanitarian Fact-Finding Commission

The Commission has been criticized as a "toothless tiger" with "limited mandate" and "no real powers."¹⁶⁴ Whereas military command investigations are limited by considerations of military efficiency, command responsibility, and individual rights, the International Fact-Finding Commission is limited by its legal competence, state consent, available resources provided to it, and geographic considerations. Article 90 provides authority for investigations only in cases of international armed conflict and only when state parties to the conflict are party to Additional Protocol I or consent to the competence of the

¹⁶¹ *Id.* § 34.

¹⁶² *Id.* § 28.

¹⁶³ *Id.* § 29; see also Protocol I, *supra* note 13, art. 90 § 5(c) ("The Commission shall not report its findings publicly, unless all Parties to the conflict have requested the Commission to do so" (emphases added)).

¹⁶⁴ Second Lieutenant Brendan Groves, *Civil-Military Cooperation in Civilian Casualty Investigations: Lessons Learned from the Azizabad Attack*, 65 A.F. L. Rev. 1, 35 (2010); see also Nout van Woudenberg, *The Long and Winding Road Towards an Instrument on Cluster Munitions*, 12 J. CONF. & SEC. L. 447, 464 (2008); Christopher Greenwood, *The Twilight of the Law of Belligerent Reprisals*, 20 NETH. Y.B. INT'L. L. 35, 37 (1989).

Commission.¹⁶⁵ Neither restriction is a fatal flaw, however, given the Commission's ability and willingness to investigate non-international conflicts, with state consent. Currently, only 71 states recognize the Commission, with the United States, Afghanistan, and Iraq among those that do not. But nothing prevents non-State parties from consenting to its competence on an *ad hoc* basis. The concern is therefore not whether the Commission currently possesses the competence to investigate civilian casualties in an armed conflict, but what incentives the United States, or a similarly situated state like Israel, might have to request or consent to the Commission's competence.

1. Risks to Consent

Non-state parties, either on whose territory civilian casualties have occurred or against whom allegations have been made, are more likely to consent to Commission competence when there is little risk to the nation itself. Risks of requesting an investigation include reciprocal investigation, loss of military assistance, and economic pressure. For instance, the government of Afghanistan could have requested a Commission investigation into the Deh Rawood incident, regardless of the U.S. national investigation. However, it would have to weigh the U.S. response to the request against any potential benefit of a Commission finding. Any dependence on U.S. military support would clearly discourage the Afghan government from pursuing such a request, unless U.S. support could be guaranteed or a Commission finding could guarantee increased safety for Afghan civilians above and beyond what the U.S. investigation might result in. Absent either, little incentive exists for Afghanistan to request a Commission investigation. Risk of consenting includes exposing the details of a military operation to an international tribunal, a potential negative finding by the Commission, and increased risk of a suit before the International Criminal Court (ICC). These must be weighed against potential international and host nation scrutiny for failure to consent.

For the United States, the risks to consent mirror the same characteristics cited by human rights advocates in support of the Commission's independence—investigating officers external to any state party to the conflict, and the Commission's existence outside the military or national command structure. External investigating officers face two obstacles: (1) the suspicion that investigations might be politically motivated against the United States; and (2) restricted access to classified information required in the course of investigation.¹⁶⁶

¹⁶⁵ See, e.g., Michael P. Scharf, *The Case For A Permanent International Truth Commission*, 7 DUKE J. COMP. & INT'L L. 375, 383 (1997).

¹⁶⁶ Groves, *supra* note 164, at 35.

The former concern parallels stated U.S. objections to the Rome Statute, fearing politically motivated prosecutions by ICC.¹⁶⁷ Based on the notion of inherent national bias, it carries no greater weight than the counterargument that a civilian casualty investigation could not be impartial because the investigating officer is American. More significant is the latter concern, which itself comprises two distinct issues.

First is physical access to classified information, which may be required in certain instances to make an informed determination about the factual situation. Current U.S. regulations require clearance from the highest levels of U.S. leadership in order to disclose certain classified information to foreign personnel. Even then, disclosure may be prohibited in order to protect intelligence gathering sources and techniques. Second is the fear of unauthorized disclosure by foreign personnel subsequent to the investigation. Whether or not malicious or even intentional, the potential exists for further dissemination of classified or other information by those over whom the U.S. has no authority or means of ensuring compliance through disciplinary proceedings.

Finally, the United States also faces a fundamental challenge due to its often disparate interpretation of use of force obligations under IHL, and the applicability of human rights norms during armed conflict.¹⁶⁸ No incentive exists to subject U.S. troops to evaluation pursuant to a legal standard post-conduct that differs from the standard in force at the time of operations (i.e. U.S. Rules of Engagement (ROE) and IHL interpretation). The IHFFC would have to limit its role to purely fact-finding in order to overcome U.S. challenge on this basis.

2. Amelioration of Risk

Although these aforementioned risks are not insurmountable, failure to ameliorate them will continue to discourage the United States from consenting to the IHFFC's competence. As suggested by national investigation procedures, many civilian casualty investigations will not require the inclusion of classified information. If inclusion is unavoidable, foreign investigators are not *per se* prohibited from access to it. Foreign coalition military leaders are routinely granted access to U.S. classified information, especially in when planning and carrying out operations, often in summarized form to prevent the disclosure of intelligence gathering sources and techniques. Chamber members could also be granted access for the limited purpose of investigating an alleged incident. Commission rules expressly prohibit unauthorized disclosure, and information sharing could be handled through diplomatic means similar to any other

¹⁶⁷ Major Kari M. Fletcher, *Defining the Crime of Aggression: Is There an Answer to the International Criminal Court's Dilemma?*, 65 A.F. L. Rev. 229, 242-44 (2010).

¹⁶⁸ See Groves, *supra* note 164, at 20-21.

violation within U.N. operations. Some military leaders have gone so far as to caution against risky operations that rely exclusively on highly classified intelligence that cannot be subsequently disclosed. For example, after U.S. officials refused to disclose intelligence information supporting a 1998 cruise missile strike on a pharmaceutical factory in Sudan, U.S. allies began questioning the strike's legitimacy. Major General Charles Dunlap, U.S. Air Force, writing after his retirement, stated "if the intelligence information is so sensitive that it cannot be disclosed, decision-makers must carefully consider whether the target should be struck at all."¹⁶⁹

The Commission's existence outside the military command structure is more problematic. The prohibition against Chamber members participating in any investigation involving their own nation would limit U.S. control over investigations of its own forces.¹⁷⁰ Although the U.S. has permitted joint investigations with the host country in the recent conflicts in Iraq and Afghanistan, it has not consented to exclusion from the process entirely. The UN accusation of a cover-up in Deh Rawood, though retracted, only exacerbates the reluctance of U.S. officials to consent to an investigation in which it plays no roll.

IV. Alternative Systems

Even those that call for the United States to employ international procedures like the Fact-Finding Commission recognize that national investigations will likely remain the predominant process by which most civilian casualty incidents are investigated.¹⁷¹ The responsibility to ensure troop and command compliance with IHL obligations lies first at the national level, while international institutions "supplement national systems of investigation and prosecution for violations of humanitarian law if national systems fail to act."¹⁷² This is due primarily to the operational capability of investigating officers from within a military command, as discussed in Part II. Their access to resources, evidence, witnesses, and locations is unrivalled compared to the limited reach of the Commission. To address the critiques of the U.S. system, it is worthwhile to first consider how alternative national and international systems operate to increase transparency and accountability while maintaining the integrity of the national system. Two that warrant a closer look—sole reliance on criminal law

¹⁶⁹ Dunlap, *supra* note 94, at 8, 18 (*citing* Department of Defense, Background Briefing, Terrorist Camp Strikes (Aug. 20, 1998), www.defenselink.mil/news/Aug1998/x08201998_x820bomb.html) (arguing "adversaries are manipulating civilian casualties to wage lawfare" against the United States, eroding public support because they cannot defeat the United States militarily).

¹⁷⁰ *Cf.* Groves, *supra* note 164, at 35.

¹⁷¹ KU & JACOBSON, *supra* note 4, at 349.

¹⁷² *Id.*

enforcement investigations and joint U.S.-host nation investigation teams—are currently in use either in other states or in a coalition environment. These alternative systems are a springboard for proposed modifications to both U.S. national investigations and the Fact-Finding Commission. The modifications address the fundamental critiques of both systems, and can propel both systems forward to greater legitimacy in investigating civilian casualties and acceptance by both sides of the debate.

A. Criminal Law Enforcement

In Schmitt's review of state practice with regard to investigations into violations of armed conflict, he describes in greater detail the concurrent criminal-administrative system adopted in four states that "enjo[y] a well-developed military justice system and [are] served by an active and well-trained judge advocate department."¹⁷³ In addition to the United States, he describes the degrees to which Canada, Australia, and the United Kingdom employ military investigations in conjunction with law enforcement investigations. In policy, all four share a similar model, allowing military administrative investigations in the absence of initial indications of IHL violations.

Canadian regulations provide for military investigation of action that is not clearly criminal, but requires that investigation be suspended upon uncovering evidence of criminality and transferred to the Canadian Forces National Investigation Service (equivalent to Army CID and NCIS in the United States).¹⁷⁴ Australian regulations likewise require a military commander initiate a Quick Assessment within 24-hours of an incident to determine what follow-on investigation is appropriate, including transfer of investigation to the Australian Defence Force Investigative Service of Australian Federal Police.¹⁷⁵ British forces similarly must initiate a Service Inquiry into potential IHL violations, and suspend and transfer the investigation to the Service Police upon determination that a crime may have been committed.¹⁷⁶ Despite the similarity in military regulations, referral to respective criminal law enforcement agencies in practice has varied widely between the United States and other states. The United Kingdom in particular, and Canada and Australia to a lesser degree, have made more prevalent use of their criminal investigative services in civilian casualty incidents. This can be attributed to both domestic policy decisions regarding

¹⁷³ Schmitt, *supra* note 17, at 56.

¹⁷⁴ *Id.* at 60. See QUEEN'S REGULATIONS AND ORDERS FOR THE CANADIAN FORCES (QR&O), chap. 21, as expanded in DEFENCE ADMINISTRATIVE ORDERS AND DIRECTIVES, 7002 series (authority to carry out administrative investigations and Boards of Inquiry (with no disciplinary consequences)); and QR&O, chap. 22 (regulatory authority for military police).

¹⁷⁵ Schmitt, *supra* note 17, at 63.

¹⁷⁶ *Id.* at 67.

such incidents, as well as states' interpretation of "use of force" obligations under international law.

1. The UK paradigm

The United Kingdom has, as a matter of domestic policy, taken the most dramatic steps to rely solely on criminal law enforcement investigations for incidences of civilian casualties. In 2003, the commander of British forces in Multi-National Division (Southeast) (MND (SE)) in Iraq established a policy that all shooting incidents were to be reported to the divisional provost marshal, upon which the Royal Military Police (RMP) would evaluate whether the use of force complied with the ROE.¹⁷⁷ If the incident was deemed to fall outside the ROE, the Special Investigation Branch (SIB) of the RMP took cognizance of the investigation. This policy, however, was reversed soon after, giving the unit Commanding Officer the discretion to determine, based on information available to them, whether military police investigation was warranted.¹⁷⁸ Only if they determined that soldiers acted outside the ROE, had doubt whether they followed the ROE, or had insufficient information to make a determination, were they required to request a law enforcement investigation by the SIB.

The investigations themselves were conducted in a manner similar to that described for U.S. command investigations in Part II. Notably different, the Commanding Officer, not investigating officer, was required to secure legal advice from the British Directorate of Army Legal Services, and opine whether the soldier acted in accordance with ROE. Their decision, advice received, and evidence relied upon were then forward to Commander, MND (SE).¹⁷⁹ However, a more crucial distinction was that if SIB had initiated a separate criminal inquiry based on independent knowledge, the unit's Commanding Officer could instruct SIB to cease its investigation.¹⁸⁰ Upon conclusion of investigation, SIB presented a report on findings of fact, without opinions or recommendations, to the unit Commanding Officer for action, rather than military prosecutors as in the U.S. system.¹⁸¹

In 2004, after substantial media scrutiny regarding a number of Iraqi civilian casualty incidents involving British forces, Commander, MND (SE) re-issued the original policy requiring that all shooting incidents resulting in civilian casualties be investigated by the SIB.¹⁸² A Brigade commander could

¹⁷⁷ *Al-Skeini*, *supra* note 30, ¶ 47.

¹⁷⁸ *Id.* ¶ 53.

¹⁷⁹ *Id.* ¶¶ 49-50.

¹⁸⁰ *Id.* ¶ 52.

¹⁸¹ *Id.* ¶ 54.

¹⁸² *Id.* ¶ 54.

only opt out of this requirement by affirmative declaration to Commander, MND (SE). This policy would be carried forward to British operations in Afghanistan in support of ISAF.

2. Application in the United States

Notwithstanding the automatic referral by British forces to the SIB, even Canadian and Australian forces are more likely than U.S. forces to refer incidents to their criminal investigation services, due to national interpretations of use of force under IHL. The military chain of command is allowed to initially determine whether evidence exists of an IHL violation. In normal combat operations, absent evidence of egregious war crimes, this usually requires determining whether troops violated the principles of discrimination or proportionality. If the commander determines that force was proportional to the military advantage, or an appropriate incident of self-defense, it reduces the likelihood of a law enforcement investigation. The more restrictive interpretations of self-defense by Canada and Australia result in a lower threshold to elevate incidents to criminal investigation. The more permissive interpretation by the United States results in a higher threshold of a referral.

A blanket U.S. policy of automatic referral of civilian casualty incidents to respective service criminal investigative divisions could address many of the same concerns that prompted British officials to reinstate their policy in 2004. Specifically, the separate chain of command and insulation from command influence could add significantly to the perception of investigatory independence. However, the sheer number of American compared to British units in combat operations make a blanket U.S. policy unworkable with existing investigative resources.

Referrals would still have to be based on some threshold criteria, although they could fall short of a positive determination or doubt as to whether the use of force was in accordance with ROE. A numerical and age threshold would minimize the discretionary aspect, currently shaped by the more permissive U.S. legal interpretation of authorized use of force. For example, referral could be automatic for any use of force incident, whether in pursuit of mission or self-defense, resulting in the death or severe injury of more than four civilians, or any child under the age of 12, unless all are positively identified as directly participating in hostilities.

However, a balance of interests must be considered before advocating for such a change in policy. Although the perception of independence would likely increase, transparency of the investigation itself would inevitably decrease due to the confidential nature of all law enforcement investigations. From a

national perspective, the increased independence may be worthwhile, given that the service criminal law enforcement divisions are a widely accepted and trusted investigation system. The long-standing tradition of the independence of these divisions, necessary in order to maintain good order and discipline within the military service, would facilitate an easy transition to a criminal system. The lack of independence of military command investigators, however, is not a foregone conclusion. Although *Al-Skeini* discussed hierarchical and institutional independence, it also stressed practical independence, which are possessed by military investigators outranking and outside the chain of command of those implicated. The perception of independence could be addressed by external guarantees. If the United States turned to strictly criminal law enforcement investigations, however, the ability to improve transparency would be greatly diminished. Criminal law enforcement investigations in the United States would not successfully address Schmitt's universal principles.

B. Joint Investigation Teams

On 22 August 2008, U.S. airstrikes in the village of Azizabad, Shindad District, Herat Province in Afghanistan killed between seven and 33 civilians, according to different U.S. investigations. Separate investigations by the Afghan government and U.N. claimed 90 civilians died.¹⁸³ In response to public outrage and government pressure in Afghanistan, the U.S. Secretary of Defense announced his intention to establish a joint U.S.–Afghan body to investigate incidents of civilian casualties.¹⁸⁴ As part of this effort, the Secretary stated that “[t]hey key for us on those rare occasions when we do make a mistake— when we do make an error—is to apologize quickly, compensate the victims quickly, and then carry out the investigation.”¹⁸⁵ Shortly thereafter, in March 2009, the U.N. Security Council passed Resolution 1868, which *inter alia* called for ISAF to conduct “investigations in cooperation with the Afghan Government in cases where civilian casualties have occurred and when the Afghan Government finds these joint investigations appropriate.”¹⁸⁶ As a result, ISAF Joint Command (IJC) established the Initial Assessment Team (IAT) concept as a joint *ad hoc* rapid response team to investigate civilian casualty allegations.

An IAT was comprised of Afghan officials from the Ministries of Interior and Defense, a coalition official from IJC in Kabul, and other staff officers, including a legal adviser, from IJC. It could and often did arrive on

¹⁸³ See Groves, *supra* note 164; see also Chronology, *supra* note 2.

¹⁸⁴ See Thom Shanker, *Gates Tries to Ease Tension in Afghan Civilian Deaths*, N.Y. TIMES (Sept. 17, 2008), http://www.nytimes.com/2008/09/18/world/asia/18gates.html?_r=0.

¹⁸⁵ See Jim Garamone, *Gates Examines Close-Air Support at Bagram*, AM. FORCES PRESS SERVICE (Sept. 17, 2008), <http://www.defense.gov/news/newsarticle.aspx?id=51214>.

¹⁸⁶ U.N. Doc. S/Res/1868, ¶ 14 (2009).

location as soon as 24 hours after the report of an incident, contingent on the security situation. Standard information-gathering procedures included receiving briefings about the operation by the involved unit, interviewing witnesses, reviewing gun-camera footage, and meeting with the local district governor's staff.¹⁸⁷ Upon completion of its initial assessment, an IAT would submit a report of the operation itself to Commander, ISAF (COMISAF) with recommendations for further action. Based on these recommendations, COMISAF could order additional investigation to determine whether the operation violated IHL obligations.¹⁸⁸ However, in part because the IAT was not bound by the due process guarantees of U.S. command investigations, these further investigations were usually conducted pursuant to the national investigation procedure described in Part II. Therefore, although the IAT may have increased the transparency of the operation in its immediate aftermath (which may have been the only intention of the concept in the first place), it did not address the accountability of the investigation process itself.

Some scholars have suggested the IAT concept could be expanded by making it a permanent body, with members to include U.N. and NGO participation, and a mandate encompassing inquiry into potential IHL violations vice merely an initial operational assessment.¹⁸⁹ This would address U.S. concerns of maintaining control of an investigation, while increasing the transparency of their procedures to some of the most vocal critics of the national system.

While an appealing option on the surface, it does not address the fundamental challenge to U.S. national investigations—the disparate interpretation of use of force obligations between IHL and international human rights paradigms. Even operating from the same set of facts, the interpretation of permissible use of force and impermissible civilian casualties under certain human rights legal paradigms is often at odds with U.S. national legal interpretation under IHL. Including NGOs in the investigative process itself would have a practical effect only in those cases where the previously undisclosed classified information was such that human rights legal paradigms would assess a military operation to meet the principles of discrimination and proportionality. As aforementioned, the majority of civilian casualty incidents do not involve such distinctive intelligence. Because evaluation of compliance with IHL obligations is not dependent on participation in the investigation, a

¹⁸⁷ Press Release, ISAF Joint Command, Lashkar Gar Evidence Points to ISAF Caused Civilian Casualties (Aug. 15, 2010), *available at* <http://www.rs.nato.int/article/isaf-releases/lashkar-gar-evidence-points-to-isaf-caused-civilian-casualties.html>.

¹⁸⁸ Press Release, ISAF Joint Command, Investigation Ordered Into Baghlan Civilian Casualty Claims (Aug. 29, 2010), *available at* <http://www.rs.nato.int/article/isaf-releases/investigation-ordered-into-baghlan-civilian-casualty-claims.html>.

¹⁸⁹ See Groves, *supra* note 164.

joint task force could only be useful in the initial assessment stages to ensure the integrity of the fact finding process. At that stage, even human rights advocates supporting use of the IHFFC do not envision the need for NGO participation. Either host nation participation through the IAT or UN participation through the IHFFC has been deemed sufficient.

Moreover, determining who should participate in a joint investigating team to increase the immediate perception of transparency depends in large part on whose perception of transparency is deemed critical. For the Afghan family member of a relative killed by military operations, there might not be anyone. Perhaps only a village elder or other trusted Afghan official (not even necessarily from the Government of the Islamic Republic of Afghanistan) (GIROA) would satisfy their perception. It is unknown how much more legitimate an investigation may appear with the additional participation of predominantly Western NGOs or the U.N. For the international human rights advocate, while the IHFFC or U.N. participation on a U.S. task force is likely sufficient, it is unknown if GIROA participation would be. Regardless, the joint investigating team can address only one part of the critique on national investigations—that of transparency. It does not address the critique of accountability.

V. A Way Forward

Understanding the challenges to the transparency and accountability of U.S. national investigations provides a foundation on which to recommend change. The perception of transparency is diminished by the perceived lack of independence of the U.S. military investigating body. That investigating body operates in an environment emphasizing military effectiveness and often issues classified reports that cannot always be shared in full with the victims or the human rights community. Accountability is primarily affected by the differing interpretation of IHL obligations and, ultimately, is judged by the prosecution (or lack thereof) for war crimes in domestic or international courts. The distinction between transparency and accountability is crucial, although the two notions are often conflated. The lack of prosecution is often viewed as a lack of transparency instead of accountability. In the alternative, the procedural system of command investigations is viewed as lacking transparency, which automatically translates to the lack of accountability. Both assumptions are flawed, however, because they presume that the integrity of the fact-finding process is dependent on the predicted outcome of the evaluation.

One scholar highlighted this distinction in his discussion of the appropriate composition of an investigating body:

[I]f the prevailing opinion were that an evaluating body would only be deemed efficient if reports were actually being evaluated, the question on the reference point for evaluation bears an impact on the composition and status of the evaluating body. I.e. if reports are to be evaluated on a factual basis, administrative as well as military experts have to be included in the body, on the governmental and/or on the non-governmental level. If reports are to be evaluated, at least additionally, on a legal basis, the participation of legal experts in the evaluating body is a natural precondition for its functioning.¹⁹⁰

Evaluation on a “factual basis” ensures both substantive and procedural accuracy in the fact-finding process. Ensuring procedural accuracy, or transparency, in turn supports the perception of a comprehensive and appropriate process to ascertain accurate facts and serve as a precondition for accountability. Transparency could be satisfied by an accurate representation of what was known and seen by participants and witnesses to the event, not distorted to reflect one particular outcome or viewpoint. Evaluation on a “legal basis” comprises part of the drive for accountability, with particular emphasis on the outcome of an evaluation to determine whether a use of force incident violated IHL obligations. While improving the perception of accountability of the entire investigation process would require confronting the divergent U.S. interpretation of IHL, improving the perception of transparency and integrity of the fact-finding process could be achieved more easily. Bearing in mind the intended purpose and audience of the investigation, modifying the procedural rules could, among other goals, put greater emphasis on apologizing to the local population, compensating victims more quickly, disclosing more information to the general public, placing greater individual liability on service members, or compiling more thorough lessons learned.

A. Changes to U.S. National Investigations

As aforementioned, the three main critiques of the national investigation system are (1) the perceived lack of independence of the appointing authority and investigating officer; (2) the perceived overemphasis of upholding military operational procedures to the detriment of a full investigation; and (3) the perceived lack of transparency of the investigation process and results. Certain procedural reform targeted to each of these concerns can increase the perception of transparency and accountability while

¹⁹⁰ Spieker, *supra* note 129, at 86.

maintaining the integrity of the U.S. national system and effectiveness of military operations.

1. The Inspector General model

One solution would be to move the responsibility for command investigations to an external authority within the existing administrative framework, like the individual service and department-wide Inspector General (IG) offices. The IG is wholly resourced by the respective service, and IG officers are given unrestricted access to all documents, witnesses, and other evidence relevant to an investigation.¹⁹¹ Because all service personnel are obligated to cooperate with IG investigations, the IG officers may receive sworn testimony and conduct questioning “consistent with Constitutional, Statutory and regulatory Due Process protections.”¹⁹² Although the resources, access, and due process guarantees are similar to command investigations, the IG’s distinction with regard to competence and authority better suit it to investigate civilian casualty incidents with more independence and less emphasis on preserving military procedures.

A foundational assumption made by many critics is that independence is impossible when the appointing authority and investigating officer are from the same military chain of command as the individual(s) being investigated. As previously discussed, legal requirements do not require such a strict separation to ensure impartiality and independence. They can be satisfied so long as the investigating officer was not personally involved and has no personal interest in the outcome of the investigation. Perception of independence, however, remains a significant obstacle to acceptance of the U.S. investigatory system.

The IG reports directly to the respective service secretary in order to assure freedom from undue command influence. Its investigating officers are all trained specifically in investigation techniques and procedures, unlike those appointed to conduct an administrative investigation as a collateral duty for the command. There is generally a full-time IG officer with supporting staff at most major Echelon II commands and above, and IG capability at Echelon III and below commands. Although the IG officer reports to a cognizant commander, she or he works independently and is expected to maintain simultaneous reporting up the IG chain of command to ensure no undue influence by the commander. The Navy policy, for example, specifically notes that, “[a]ll inquiries into matters affecting the readiness, integrity, discipline, and efficiency

¹⁹¹ This applies to evidence classified through SECRET. Spaces and information classified at a higher level may be released after further clearance has been established.

¹⁹² See, e.g., U.S. DEP’T OF NAVY, SEC’Y OF NAVY INSTR. 5430.57G, MISSION AND FUNCTIONS OF THE NAVAL INSPECTOR GENERAL ¶ 5 (2005) [hereinafter SECNAVINST 5430.57G].

of the DON shall be conducted in an independent and professional manner, without command influence, pressure, or fear of reprisal from any level within DON.”¹⁹³ When circumstances “place the independence or impartiality of the inquiry in doubt,”¹⁹⁴ the IG is required to refer the matter up the IG chain of command, or to the service Secretary for external investigation.

The IG process also specifically challenges the assumption that upholding the operational status quo maintains military effectiveness. It already routinely handles investigations of command procedure, often initiated either by “whistleblowers” or third-parties outside the military system, and enjoys a greater reputation for critical assessment of standard military procedures.¹⁹⁵ Although the IG is commonly known for its auditing function, it has also traditionally investigated service and command professional ethics. For example, the Naval IG office describes itself as “the conscience of the Navy,” responsible for inspecting, investigating, or inquiring into any matters of importance to the department, in order to maintain “the highest level of integrity and public confidence.”¹⁹⁶ The Naval IG distinguishes the mandate of NCIS, which “focus(es) on individual criminal activity,” from its own, to investigate “the effectiveness of command procedures for good order and discipline or the effectiveness with which command personnel have carried out their duties.”¹⁹⁷ Included among the matters for investigation that are explicitly within its core mission are military readiness, effectiveness, efficiency, discipline, ethics and integrity.¹⁹⁸ The presumption for the IG is not to preserve existing operational procedures, but rather to question whether such procedures are in fact the most effective and ethical.

The major obstacle to effectively using the IG for civilian casualty investigations is the final report and publication. Although the IG routinely releases its reports within the service, and FOIA is technically applicable, a specific exemption from release is made for IG reports. For example, the Navy policy reads:

The NAVINSGEN is the confidential agent of SECNAV, CNO, and CMC for obtaining uninhibited self-analysis and self-criticism of the internal management, operation, and administration of DON. Therefore, NAVINSGEN reports are

¹⁹³ *Id.*

¹⁹⁴ *Id.* ¶ 7(p).

¹⁹⁵ *Id.*

¹⁹⁶ NAVAL INSPECTOR GENERAL, <http://www.secnav.navy.mil/ig/Pages/Home.aspx> (last visited June 28, 2015).

¹⁹⁷ SECNAVINST 5430.57G, *supra* note 192, ¶ 7(c).

¹⁹⁸ *Id.* ¶ 8.

internal memoranda and constitute privileged information that is not releasable outside DON except with specific approval of NAVINSGEN.¹⁹⁹

While the service IG may coordinate and clear publication on exception, the general policy is one of non-disclosure. This stands in distinct contrast to command investigations, which have no such prohibition. In order to achieve uniform publication of investigation results, the Secretary of Defense would have to issue a new policy specifically exempting civilian casualty investigations from non-disclosure. In the alternative, the policy could be to publish unclassified summaries of the final reports. While not impossible, the political pressure needed to alter a fundamental practice of such a long-standing process would likely be enormous. However, if the military believes the perception of effective investigations are critical to successful counterinsurgency campaigns, as was the case in Afghanistan, then the modification to the disclosure rules of an otherwise well-suited investigatory system may not only be justified but also critical.

2. The Higher Authority Model

A less ideal solution would be to move the responsibility for command investigations not to an external authority, but simply to a higher authority, within the existing administrative framework. Instead of appointing an investigating officer from the same command as the individuals under investigation, they could be appointed from the general court-martial convening authority (GCMCA) level or higher. In order to remove any discretionary aspect from the unit level, all civilian casualties, regardless of reason, would be reported up to the GCMCA level for determination of preliminary inquiry and further investigation. The GCMCA already routinely handles matters for subordinate commands when disciplining senior leadership of a unit. Unless the GCMCA was involved in ordering the conduct under question, this would remove any likelihood of personal interest in the outcome of the investigation. It could also incorporate host nation officials into joint investigations as standard procedure to further increase the perceived impartiality of the investigating body. Such an investigation would maintain all the other benefits of a command investigation, including access to resources and evidence, due process guarantees for service members, and public disclosure of the final report through FOIA requests.

Although not prohibited from doing so, the GCMCA lacks the IG's mandate to critically question operational procedure, and may be as susceptible

¹⁹⁹ *Id.* ¶ 9.

a perception of upholding the military effectiveness status quo just like command investigation ordered at a lower level. Therefore, a GCMCA-level investigation would have to compensate for this challenge by strongly counteracting the third critique of the national system—post-investigation transparency. Just as the theater commander in Afghanistan instituted a new policy to track all civilian casualties, he could require as standard practice the publication of unclassified summaries of all civilian casualty investigations, such as in the Deh Rawood incident. This would enable discovery and dialogue with family members personally affected by military operations, as well as facilitate NGO efforts to track casualty trends and response measures without having to bring them into the investigative process itself.

The major challenge to GCMCA-level investigations would be the strain on resources. Instead of having investigative responsibility for the conduct of only one unit with potentially no more than several hundred service members, the GCMCA command would have investigative responsibility for the conduct of multiple units, potentially consisting of several thousand soldiers. This could significantly detract the GCMCA and the appointed investigating officer from their operational responsibilities. This becomes a matter of resources and manning, however, and not an issue about the merits of creating a new institutional solution. The procedures, directives, and familiarity with GCMCA-level investigations are already embedded within the U.S. system. The effort to increase manning to a GCMCA for the express purpose of conducting civilian casualty investigations during a specific armed conflict is neither entirely novel nor impractical to demand. Without having to create an entirely new procedure, these reforms could be implemented fairly quickly and could begin to address some of the greatest critiques against the U.S. national investigation system.

B. Changes to the International Humanitarian Fact-Finding Commission

The above solutions may be insufficient for instances in which the operation under investigation was planned and approved at a level significantly high enough to call into question the impartiality of any investigator within the military. These would most likely be large scale air-strikes coordinated between services. Even if the IG non-disclosure policy was altered, or the GCMCA-level investigation provided adequate summaries of every civilian casualty investigation, the transparency of the process in this circumstance might be insufficient to counter criticisms of the investigating officer's independence. Whether accurate or not, a perception of personal interest in the outcome of the investigation could be attributed to the highest echelons of military and civilian leadership. In that circumstance, an investigating body such as the IHFFC could still prove useful to supplement the national system on an *ad hoc* basis. U.S. consent to its competence, however, would depend on whether modification of

procedure would be sufficient to counter the major sustaining critiques of the IHFFC—the lack of U.S. participation and divergent interpretations of IHL.

1. Modifying Membership Rules

From the U.S. perspective, Chamber membership would ideally be revised to include at least one national of the state party to the conflict. This would ensure that the U.S. perspective, for instance, was taken into account when investigating the conduct of its troops. The IHFFC's procedural guidelines, however, cannot be modified as easily as the national system. Chamber membership is explicitly provided for in Article 90 of API, and any revision to this rule would require amendment by a majority of state parties to the Protocol. A fundamental tenet of the Commission²⁰⁰ was this non-party requirement, making modification to include representation by a party to the conflict highly unlikely. Even if the rules could be modified, inclusion of one voting member from a state party to the conflict would be insufficient to guarantee acceptance of that perspective. The majority of Chamber membership could still overrule one representative. In fact the intent of the rules is to ensure no one national perspective dominates the investigation.

2. Standardizing Investigation Procedures

A more feasible solution would be to standardize investigation procedures and findings to minimize the potential impact of politically motivated results or divergent interpretation of IHL standards.²⁰¹ For instance, the relative credibility of witness statements could be evaluated according to pre-established neutral criteria, such as requiring corroboration and sworn testimony, and disallowing use of compensated statements. Guidelines must also limit the extent to which the Chamber may draw conclusion on the basis of accusations that cannot be independently verified, regardless of the accused state's ability to produce evidence to the contrary. The investigation could also explicitly detail the steps taken to gather and verify witness statements in order

²⁰⁰ The ICRC Commentaries on Protocol I, Article 90 further elaborates that "it would seem not only desirable that the members of the Chamber are not nationals of a Party to the conflict, as stated in the text, but that they belong to neutral countries. The two 'ad hoc' members . . . 'represent' the Party which has appointed them and should contribute to creating an atmosphere of trust within the Chamber itself." CLAUDE PILLOUD ET AL., COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 ¶¶ 3631-3632 (Yves Sandoz et al. eds., 1987) (commenting on Additional Protocol I, Article 90(3)(a)).

²⁰¹ Although the United States is often critiqued for its reliance on political ill-motivation as a justification against consenting to the competence of the IHFFC or ICC, Judge Goldstone noted as much against Israel during his 2009 investigation into the Gaza conflict. He stated, "I insisted on changing the original mandate adopted by the Human Rights Council, which was skewed against Israel." See Goldstone Report, *supra* note 24.

to provide the opportunity to rebut or independently verify such statements. Adherence to elevated standards of proof, including a presumption in favor of compliance with IHL obligations and protection of witnesses during questioning, commensurate with U.S. due process guarantees would also improve the acceptability of the IHFFC process. Finally, any recommendations would have to explicitly reference the legal standard used to evaluate the incident, noting any divergence in legal interpretation between the nation under investigation and the standard used in the investigation.

3. Lessons Learned: The Goldstone Report

Drawing lessons learned from critiques of the Goldstone Report,²⁰² the methodology of investigation remains a critical factor in the acceptability of an investigative report.²⁰³ Among the critiques most often levied against the report was that it inferred an intention on the part of the Israeli military, in violation of IHL obligations, based on isolated incidents. The report failed to distinguish between an intention to specifically target civilian infrastructure, which may be permissible under certain conditions, and the impermissible intent to kill civilians. Despite its stated contention that it was not a judicial or quasi-judicial proceeding, the Goldstone Report was interpreted by many as a significant condemnation of the Israeli military for a policy of intentionally killing civilians. While the confidentiality of IHFFC reports significantly mitigates this concern, the possibility of release means it must take precautions against inferring a national policy without specific evidence of the promulgation of such a policy.

Moreover, the allegations investigated by the Goldstone Report were of such a nature that credible evidence existed to rebut such accusations but was not pursued in the course of the investigation. In his recent response piece, Judge Goldstone lamented the lack of Israeli participation in the investigation, to which he attributes the majority of the report's failings:

The allegations of intentionality by Israel were based on the deaths of and injuries to civilians in situations where our fact-finding mission had no evidence on which to draw any other reasonable conclusion Although the Israeli evidence that has emerged since publication of our report doesn't negate the tragic loss of civilian life, I regret that our fact-finding mission did not have such evidence explaining the circumstances in which we said civilians in Gaza were targeted, because it

²⁰² Goldstone Report, *supra* note 24.

²⁰³ Alan Dershowitz, *The Case Against the Goldstone Report: A Study in Evidentiary Bias* (Harvard Law School, Public Law & Legal Theory Working Paper Series, Paper No. 10-26), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1542897##.

probably would have influenced our findings about intentionality and war crimes. . . . Israel's lack of cooperation with our investigation meant that we were not able to corroborate how many Gazans killed were civilians and how many were combatants.²⁰⁴

The lack of evidence upon which to draw an alternative conclusion, however, is not equivalent to sufficient evidence upon which to support the allegation. The fact that the Goldstone panel could conclude that the allegations were supported despite the lack of critical evidence from a key party to the conflict reflects a fundamental concern of the United States with regard to the international investigation process. The IHFFC would have to create an *ex ante* rule, agreeing to limit its conclusions if the state against which allegations are made cannot provide rebuttal evidence (for instance, due to classification or intelligence purposes).

Ultimately, Judge Goldstone limited the impact of his own report, stating that the primary recommendation “was for each party to investigate, transparently and in good faith, the incidents referred to in our report. . . . The purpose of these investigations, as I have always said, is to ensure accountability for improper actions, not to second-guess, with the benefit of hindsight, commanders making difficult battlefield decisions.”²⁰⁵ This sentiment echoes other scholars who have advocated for limits on the direct impact of expert committees or special commissions, vice action by a sovereign or a majority of state parties to a treaty.²⁰⁶ An express recognition of this principle by the IHFFC, both in its mandate and preamble to any investigation, would demonstrate the IHFFC's role as a supplement to the national investigatory system. This would lessen the U.S. grounds for objection if the stated purpose is to identify incidents for further response, rather than serve as a precursor to prosecution in the ICC.

VI. Conclusion

In a counterinsurgency, such as the one recently fought in Afghanistan by U.S. and Coalition forces, the reaction of the populace in response to military operations is arguably as important as the operations themselves. While the prevention of civilian casualties is of primary importance, transparent and

²⁰⁴ Richard Goldstone, *Reconsidering the Goldstone Report on Israel and war crimes*, WASH. POST (Apr. 1, 2011), http://www.washingtonpost.com/opinions/reconsidering-the-goldstone-report-on-israel-and-war-crimes/2011/04/01/AFgl11JC_story.html.

²⁰⁵ *Id.*

²⁰⁶ See, e.g., Spieker, *supra* note 129, at 86 (“[l]astly, should a voluntary reporting system in international humanitarian law result in any form of a non-compliance reaction, such decisions will not be conferred to an expert committee or group body, but would have to be taken by a plenary of member states”).

legitimate investigation of incidents that do occur contributes equally to “winning hearts and minds.” Civilian casualties have traditionally been investigated through national channels, whether administrative or criminal in nature, as have the subsequent disciplinary measures. But in recent years, with a rise in civilian casualties due to air-strikes and artillery fire, human rights advocates have increasingly called for the international community to take up the mantle of investigation. Specifically, many critics have called for the utilization of the IHFFC, as provided for in Additional Protocol I to the 1949 Geneva Conventions. Opponents in the United States, which has not ratified API, have resisted efforts to compel consent to the competence of the IHFFC in its present form.

This produces a stalemate between proponents of the national system and proponents of the IHFFC. In order to begin to approach a common ground, the two systems must be compared in greater detail to determine where the points of similarity and divergence are. Rather than view the procedures as competing systems, they can be seen as complimentary aspects of a highly nuanced environment.

Part I established the relative lack of international guidance on the form and procedure of civilian casualty investigations. From the brief survey of customary international law, treaty standards, and judicial precedent, the major principles for investigations appear to be transparency and accountability. These have alternately been described in the Goldstone Report as independence, impartiality, effectiveness, and promptness. Distinguishing investigations from subsequent prosecution or disciplinary measures, the key principles are more accurately independence and transparency.

Using this guidance, Part II explored the benefits and obstacles to acceptance of the national investigation process in the United States. Of primary benefit are the immense resources and access to evidence inherent in the U.S. process, in addition to the due process guarantees given to service members during an investigation. Although administratively cumbersome, the ability to retrieve results of investigations after completion of disciplinary proceedings through the FOIA process is critical to the transparency of the system. Although many critics cite the bureaucratic hurdles to obtaining information under FOIA, the legal guarantee of ultimate access to such information cannot be overstressed. Most troublesome in the U.S. system is the perceived lack of independence due to the method of appointing an investigating officer and lack of transparency if a FOIA request is not made.

Part III compared the IHFFC to the national process, identifying similarities and differences that either strengthened or weakened the justification

for relying on national investigations. Surprisingly, the IHFFC can be considered somewhat less transparent than national investigations, since publication of the findings is dependent on national consent of all parties to the conflict. Lacking the same resources, access to evidence, and due process guarantees, the IHFFC's strength lies in the purported impartiality of its investigating body. The IHFFC's mandate seems to be based solely on the national neutrality of the investigating Chamber, which draws its members from multiple disciplines, including military expertise. From a U.S. perspective, the greatest critique is the inability for the United States to participate, let alone influence, any investigation of its own troops. Furthermore, the divergent interpretation of IHL obligations between the United States and others in the international community discourages U.S. consent to subject its military forces to investigation under a legal standard it does not subscribe to. This also encourages U.S. objections to politically motivated investigations made in bad faith.

Given these setbacks, Part IV considered possible alternatives to the national system that might address the independence and transparency claims at the foundation of the call to use the IHFFC. The criminal law enforcement model used in the United Kingdom, while squarely addressing the independence concern, would decrease the transparency of the system. The confidentiality of law enforcement investigations, mandated to preserve the trial process, would defeat the efforts to increase transparency of the investigation process. Bringing in host nation officials through the joint investigating team concept could be more promising. A joint effort could increase the transparency of the fact-finding portion of an investigation, although not necessarily the subsequent accountability. Depending on who is evaluating the process, however, subsequent accountability may be less important than immediate information and acceptance of responsibility by military forces in general.

Given the problems of the existing alternatives, feasible changes to the national investigation system include transferring the responsibility for investigation up or outside the chain of command, and regularly publishing full results or, as required, unclassified summaries of investigation results. Ideally, the responsibility could shift to the service IG's office, which is already specifically mandated to conduct independent review of existing military procedures. To do so, however, would require a Department of Defense-wide policy that would allow the publication of the investigations or summaries. Although this would address both the independence and transparency of investigations, the critical departure from the "self-criticism" function of the IG may be politically too difficult to overcome. Alternatively, raising the responsibility to investigate incidents to the GCMCA would achieve some increase in the independence of the investigating officer. The significant level of

congressional oversight of Flag Officer promotions would guarantee civilian oversight over those GCMCA's with cognizance of especially egregious incidents. This would also allow easier implementation of a policy to publish unclassified summaries, without waiting for a FOIA request, in order to proactively inform families and NGOs of the course of events. These modifications would begin to address the strongest critiques against the U.S. investigatory process—namely, the lack of transparency and independence.

Even with these changes, U.S. investigations may not always be the most preferred recourse for a civilian casualty incident, especially those implicating higher echelons of command. In these instances, the IHFFC poses a useful supplement to the U.S. system. Changes to the IHFFC are more prescriptive in nature, attempting to establish a strict standard for the pursuit and use of witness statements. The proposed changes are aimed at ensuring that any failure of a state party to respond to requests for evidence would be noted appropriately, as opposed to grounds for substantiating an allegation. The critiques of the Goldstone Report methodology highlighted the need to ensure the accuracy and limits of an allegation, despite the lack of contrary information. Establishment of *ex ante* rules to address witness and evidence collection is crucial, especially to lay out the procedural treatment of evidence inequality.

With these proposed modifications, an integrated system using the IHFFC to supplement national investigations would benefit three constituencies: the local populace, U.S. national interests, and international human rights interests. The unclassified summaries would serve to quickly disseminate information to families of victims, while allowing U.S. control of the process on an immediate level. A policy of tracking and conducting at least preliminary inquiries into every incident would also increase the uniformity and predictability for locals and others directly affected by military operations. Unlike the uncertainty of the system now, as expressed by Alston, locals could be assured that an investigation occurred and that they would be apprised of at least a summary of events at the conclusion of the investigation. Resort to the IHFFC would be reserved for those cases in which the needs of the local populace are possibly secondary to the international critique. Without having to resolve the debate over the extraterritorial application of human rights law in armed conflict, these changes demonstrate that the national investigatory process can still satisfy underlying human rights principles while adhering to a traditional IHLS standard. These practical steps can be implemented immediately in order to address the fact-finding needs of those most affected – the families of those civilians killed in armed conflict.

BOOK REVIEW

Major Alex M. Straub, ARNG*

*Forces of Fortune: The Rise of the New Muslim Middle Class
and What It Will Mean for Our World*¹

“Where there is an interest in business, there is an impulse toward moderation and order over extremism and chaos.”²

I. Introduction

In his book, Dr. Vali Nasr proposes new policy directions for the West to effectively engage with the Muslim world in the Middle East. Not only does he believe that United States’ policy over the years has been largely ineffective at tackling extremism in the region, but also that it is actually impeding the region from emerging into the “rapidly changing global environment,” which, in his opinion, is the way for the Middle East to emerge from its current state of fanaticism, violence, and instability.³ His argument is that sanctions, misplaced military action, and support of authoritarian regimes—all while preaching democracy—might not be the best avenues of engagement to help the region reach goals of stability and “modernity” and extinguish Islamic extremism.⁴ For him, the West must engage the Middle East on another level—an economic level—and with different players: the Muslim middle class.

According to Nasr, only by engaging the “true bourgeoisie” or “middle class” of businessmen and professionals, such as lawyers, doctors, and writers—

* Judge Advocate, U.S. Army National Guard. Presently assigned as Joint Staff Legal Advisor, Joint Forces Headquarters, Washington (Army & Air) National Guard, Tacoma, Washington. LL.M., 2011, The Judge Advocate General’s School, U.S. Army, Charlottesville, Virginia. J.D. 2005, Seattle University School of Law; B.A., 2001, Central Washington University. Previous assignments include Brigade Judge Advocate, 81st Armor Brigade Combat Team, Seattle, Washington, 2013-2015; Foreign Claims Commissioner and Contract & Fiscal Law Attorney, 4th Infantry Brigade Combat Team, Afghanistan, 2013; Operational Law Attorney and Trial Counsel, Joint Forces Headquarters, Washington Army National Guard, Tacoma, Washington, 2006-2010.

¹ VALI NASR, *FORCES OF FORTUNE: THE RISE OF THE NEW MUSLIM MIDDLE CLASS AND WHAT IT WILL MEAN FOR OUR WORLD* (2009).

² *Id.* at 168.

³ *Id.* at 86.

⁴ *Id.* at 1-3.

especially those operating independently from government sponsorship—will democracy and capitalism prevail.⁵ In Nasr's rather simplistic terms, "[f]ueling the activities of the Middle East's rising middle class . . . can push the status quo to the tipping point where national leaders have no choice but to embrace change That is the key step toward liberalization of the political systems."⁶ This economic force will be the driver of societal reforms in many areas and will eventually bring true stability and democracy to the region, avows Nasr.⁷

II. About the Author

Dr. Vali Nasr is a highly respected scholar on Middle Eastern affairs⁸ and his credentials are quite impressive: Dean of the School of Advanced International Studies at Johns Hopkins University; Senior Advisor to the Special Representative for Afghanistan and Pakistan (Richard Holbrooke); Professor of International Politics at Tufts University; Senior Fellow at Harvard University; Adjunct Senior Fellow at the Council on Foreign Relations; and Professor at the Naval Postgraduate School.⁹ Additionally, he has been published extensively, testified to Congress on Middle Eastern affairs and served as an adviser to the U.S. President, Vice-President, Secretaries of State and Defense.¹⁰ Nasr is also a Carnegie Scholar and has appeared on many popular news outlets, including "CNN, the BBC, National Public Radio, and not least of all *The Daily Show with Jon Stewart* and *The Colbert Report*."¹¹

The author has a personal connection to the Middle East that provides a unique perspective to his book. Nasr was born in Iran and immigrated to the United States with his family after the Iranian Revolution in 1979.¹² Nasr's family had lived in Iran for many generations and in his book he draws from many of their experiences in Iran preceding its revolution.¹³ It is apparent the author still maintains his significant ties to the Middle East, its people and culture, as his references to extensive travels to the region for research and conducting interviews evinces.¹⁴ These factors tend to lessen any impression that

⁵ *Id.* at 85.

⁶ *Id.* at 26.

⁷ *Id.*

⁸ See, e.g., Paul Barrett, *Can Entrepreneurs Tame the Mideast?*, BUS. WEEK (Sep. 10, 2009), http://www.businessweek.com/magazine/content/09_38/b4147077174583.htm (referring to Nasr as "an eminent Middle East scholar").

⁹ Vali R. Nasr, Ph.D., JOHNS HOPKINS SCHOOL OF ADVANCED INTERNATIONAL STUDIES, <https://www.sais-jhu.edu/vali-nasr> (last visited June 26, 2015).

¹⁰ *Id.*

¹¹ Vali Nasr: Professor of International Politics, Tufts University, BIG THINK, <http://bigthink.com/experts/valinasr> (last visited June 26, 2015).

¹² *Id.*

¹³ NASR, *supra* n.1, at 110–12.

¹⁴ See, e.g., *id.* at 232.

the book was written from a purely academic perspective and acknowledges that the author has a personal stake in the region and its fate.

III. Analysis

A. “The Power of Commerce”¹⁵

For those not entirely familiar with the Middle East, Nasr graciously begins his book with a helpful recounting of major events that have taken place since 1978 and have shaped the region’s current state.¹⁶ From there, he attempts to dispel what he believes are common misconceptions of the region often held by Westerners, such as beliefs that radical Islamic fundamentalism is on the rise¹⁷ and that Islam is not compatible with modern economic systems.¹⁸ In response to the latter, Nasr begins by focusing on the growing consumerism of the Muslim world and its appetite for Islamic goods and services and access to Islamic financing options.¹⁹ His elaboration on the Islamic finance system is quite insightful for readers not familiar with the region’s economic system and he explains certain peculiarities that are not present in Western financial systems.²⁰ He also mentions how this growing Islamic finance sector has attracted many large and well-known Western banks to invest in the region and offer tailored financial services, including Islamic bond and investment funds.²¹

The first chapter of the book outlines the author’s general thesis: that as more and more Middle Easterners enter the ranks of the middle class by becoming owners and leaders of private-sector businesses they are embracing capitalism and endeavoring to join the larger global economy; eventually, Nasr states, this capitalist revolution will leave the region’s leaders no choice but to

¹⁵ *Id.* at 1. This term is the title of the first chapter and is used here to highlight his theme.

¹⁶ *Id.* at 1–10.

¹⁷ *Id.* at 10. Unfortunately, the author does not cite a study or otherwise provide a source for this assessment.

¹⁸ *Id.* at 15.

¹⁹ *Id.* at 14. The author lists “Islamic housing, haute couture, banking, education, entertainment, media, consumer goods (such as Europe-based alternatives to Coke and Pepsi, Mecca Cola and Qibla Cola), and even vacations” as examples of Islamic goods and services.

²⁰ *Id.* at 16. The author describes Islamic financing as loans, banking products, and investment vehicles that comply with “Shariah” rules and regulations, such as not charging interest on loans and avoiding investment in “businesses that serve alcohol, involve gambling, produce devices that can promote immorality, or in some cases, even the use of mannequins or bareheaded women in advertising.”

²¹ *Id.* at 17 (referencing “HSBC, Deutsche Bank, Barclays, Credit Suisse, Citigroup, and the UK’s Black Rock” as examples of Western banks operating in the Middle East).

embrace progress and reform that will lead to a liberalization of rights and eventually democracy in the region.²²

B. Roots of the Original Muslim Middle Class

Nasr provides a comprehensive account of the Muslim middle class's origins which he asserts largely came about by early Muslim captivation with a seemingly more modern and secular European state.²³ Eventually, this fondness of European ways gave birth to a new Middle Eastern middle class in the early 20th century.²⁴ Unfortunately, for reasons cited in the book, this early middle class did not gain the same prominence as their European counterparts and were therefore unable to bring about the same capitalist and democratic reforms that occurred in the West.²⁵ Nasr cites that the primary failing of the early middle class resulted from its dependence on authoritarian regimes that endeavored to modernize their countries by imposing harsh rule and secular reforms while attempting to suppress the role of Islam within the state, breeding great discontent amongst the masses.²⁶ Nasr's dissection of this complex and unique Middle Eastern paradigm is informative and helpful to any reader seeking a deeper understanding of the region's dynamics.

C. The Middle Class and Islamic "Piety"

Nasr offers insightful coverage of the current state of Islam in the region. He describes a resurgence of Islamic "piety" that rejects "violence and extremism," as gaining favor with the Middle Eastern middle class.²⁷ Nasr's message here is quite clear: "We have to face the fact that the new Middle East being reshaped by the rising middle class is going to be—at least in the short run—Islamic."²⁸ Nasr explains that while this middle class is indeed growing more "pious," it rejects fanaticism in favor of a stable business environment and believes Islam is compatible with modernity.²⁹

²² *Id.* at 24–26.

²³ *Id.* at 90.

²⁴ *Id.* at 94.

²⁵ *Id.* at 111–12.

²⁶ *Id.* at 106–14.

²⁷ *Id.* at 176.

²⁸ *Id.* at 259.

²⁹ *Id.* at 197.

D. Dubai

The tiny emirate of Dubai, with its ultra-modern architectural “attractions” and a “skyline that competes with those of New York and Shanghai,”³⁰ is Nasr’s first example of the emerging economic power in the Middle East. Most important to Nasr’s analysis here is that Islam thrives in this very wealthy and technologically sophisticated place. Dubai, with its upscale mosques and ardent adherence to Islamic values, is a Muslim “dreamland” and the place “. . . where most Muslims claim they would like to live, other than their own country.”³¹

Unfortunately, the example of Dubai seems to work against Nasr’s theory. While Dubai has definitely embraced capitalism, it has no political parties or other mechanisms that would currently support democracy in the country.³² Additionally, it is not a bastion of progressive social values or even reform; in fact, it has been criticized for its human trafficking and violence against women, and its government restricts free speech, especially when it is derogatory to Islam or the government.³³ While it may be a bastion for businessmen—and even a good example of Islamic compatibility with the practice of business—it might not be the model some would like the rest of the Middle East to emulate.

E. Iran

Nasr refers to Iran as “an enigma, a land of puzzling contradictions.”³⁴ For those not familiar with this country or its history, Nasr’s comprehensive coverage is very insightful, especially his examination of its (past and present) political and religious machinations. Nasr provides an expose of the current Iranian regime and its personalities and ascension to the top pinnacles of Iranian power. Nasr is very thorough in his explanation of Iran’s theocratic constitutional and governmental structure, including analysis of the Iranian Revolutionary Guard’s ever expanding role in Iran’s politics and economy. This current governmental construct is important to understand, as are the circumstances that lead to its origination after the 1979 Iranian Revolution,

³⁰ *Id.* at 28–29.

³¹ *Id.* at 29–31.

³² U.S. DEPT. OF STATE, 2009 HUMAN RIGHTS REPORT: IRAN (Mar. 11, 2010), <http://www.state.gov/g/drl/rls/hrrpt/2009/nea/136068.htm>.

³³ *Id.* at 27.

³⁴ NASR, *supra* note 1, at 50.

which Nasr covers in great detail in his chapter titled: “The Great Islamic Revolution.”³⁵

Obviously, Nasr focuses much attention on the Iranian middle class, who, in his opinion, were mostly unwitting supporters of the revolution in 1979 and unaware of its ultra-radical Islamic component prior to its fruition.³⁶ Interestingly, it is this middle class, with their supposed new-found entrepreneurial spirit, on which Nasr pins his hope of turning things around in Iran.³⁷ Nasr’s predictions appear to bear out to some extent, as exemplified by the “Green Movement”³⁸ protests which followed the disputed Iranian 2009 presidential elections where Ahmadinejad defeated reformist candidate Mir-Hussein in an election many cite as neither free nor fair.³⁹ However, Nasr warns that Western sanctions do not help this “process” along and may only continue breeding resentment of the West.⁴⁰

F. Pakistan & Turkey

Nasr attributes much of Pakistan’s troubles to the overarching control of the country by its military and corrupt dictatorships. His examination of military influence and control over political affairs is quite enlightening, especially in the context that these military leaders do not always see the value in capitalist systems nor do they obviously appreciate democracy if they are exerting control over the government. However, Nasr’s assessment that the Pakistani middle class is overwhelmingly in favor of reform, including democracy, is quite optimistic—maybe too much so; he cites the “Lawyers’ Movement” that was successful in forcing some limited governmental changes in 2008 and 2009 as an example.⁴¹ Unfortunately, as even Nasr admits, Pakistan’s issues are very great, so it appears it will take a lot more than a small group of lawyers to turn things around.⁴²

It becomes very clear when reading the chapter on Turkey that Nasr believe this country really exemplifies the power of the rising Muslim middle

³⁵ *Id.* at 116.

³⁶ *Id.* at 118.

³⁷ *Id.* at 82–84.

³⁸ Thomas Erdbrink, *A Year After Its Rise, Iranian Protest Movement Stymied and in Disarray*, WASH. POST, Jun. 11, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/06/10/AR2010061004862.html>. While this movement has apparently been thwarted—at least for the moment—much of its impetus was apparently a result of middle class discontent amongst other things.

³⁹ U.S. DEPT. OF STATE, *supra* n.32, at 1.

⁴⁰ NASR, *supra* n.1, at 83–84.

⁴¹ *Id.* at 226–228.

⁴² *Id.* at 229–230 (acknowledging that the “economy has begun to unravel,” the country faced bankruptcy, and the “government is failing and the Taliban are knocking on the door”).

class and provides hope for stability and reform for the rest of the region. He specifically focuses on the emergence of the ruling “AKP” party, an Islamic party that professes to support liberal economic policies and membership in the European Union; he also cites the major growth of “Turkish entrepreneurs [who] do business directly with European and American companies and are sensitive to global economic trends.”⁴³ According to Nasr, “If Turkey stays on its course, it will become a Muslim capitalist democracy, and the face of Turkish modernity today will become the face of the wider Muslim world tomorrow if the rising business leadership and its attendant new middle class get their way.”⁴⁴

IV. Conclusion

This book has considerable value for anyone, including judge advocates and military officers, seeking to gain a deeper understanding of the underpinnings that shape the Middle East’s political, economic, religious, and social realities. Nasr’s analysis is very comprehensive and he eloquently relates the information in a manner that is easily digested by the reader. Nasr shrewdly forces readers to delve into the region’s history, analyzes the important figures and major turning points, then highlights the lessons to be learned. He also examines the effects of current and past Western policies and suggests new policy directions that might bring about more favorable outcomes for the region’s future.

While one might expect a book on such a volatile region to be filled with “doom and gloom,” Nasr inspires optimism that this region can eventually emerge from its current state of morass and eventually become a global partner with the rest of the world. While some other reviewers have interpreted Nasr’s book as being somewhat overly optimistic and unrealistic,⁴⁵ this reader believes Nasr strikes a balance that is necessary to keep the book interesting, informative, and encouraging.

⁴³ NASR, *supra* n.1, at 244.

⁴⁴ *Id.* at 250-51.

⁴⁵ See, e.g., Barrett, *supra* n.8 (stating “as soon as Nasr’s theory encounters reality, it begins to crumble”); Kaveh L. Afrasiabi, *A Flawed Picture*, ASIA TIMES, (Jan. 23, 2010), http://www.atimes.com/atimes/Middle_East/LA23Ak01.html (referring to Nasr’s book as a “romanticization[sic] . . . that paints a triumphant and rosy picture of the middle class”).

BOOK REVIEW

Major Timothy W. Thomas, USA*

*The Good Soldiers*¹

“You cannot qualify war in harsher terms than I will. War is cruelty, and you cannot refine it; and those who brought war into our country deserve all the curses and maledictions a people can pour out.”²

I. Introduction

“So I’ve committed more than 20,000 additional American troops to Iraq. The vast majority of them—five brigades—will be deployed to Baghdad.”³ With these words, President George W. Bush began an escalation of the war in Iraq that would come to be called “the surge.”⁴ While the wisdom of this decision was debated in Washington D.C. and around the country,⁵ the troops tasked with accomplishing the mission were set to work.

* Major (MAJ) Thomas is a judge advocate in the U.S. Army. Presently assigned as the Deputy Chief, Defense Counsel Assistance Program, United States Army Trial Defense Service, Fort Belvoir, Va. LL.M., 2011, The Judge Advocate General’s Legal Ctr. & Sch. (TJAGLCS), Charlottesville, Va.; J.D., 2001, University of Houston Law Center, Houston, Tex.; B.A., 1998, University of Texas–El Paso, El Paso, Tex. Previous assignments include: Chief of Military Justice, Fort Leonard Wood, Mo. 2011–2013; Appellate Attorney, Defense Appellate Division, United States Army Legal Services Agency, Arlington, Va. 2008–2010; Senior Defense Counsel, Fort Leavenworth, Kan. 2005–2008; Defense Counsel, Balad, Iraq, 2004–2005; Defense Counsel, Fort Riley, Kan. 2003–2004; Chief, Legal Assistance, Fort Riley, Kan. 2003; Legal Assistance Attorney, Fort Riley, Kan. 2002–2003. Member of the bars of Texas, the U.S. Army Court of Criminal Appeals, the U.S. Court of Appeals for the Armed Forces, and the U.S. Supreme Court.

¹ DAVID FINKEL, *THE GOOD SOLDIERS* (Sarah Crichton Books 2009).

² General William T. Sherman, Orders to the Mayor and City Council of Atlanta (Sep. 12, 1864), available at http://www.sewanee.edu/faculty/Willis/Civil_War/documents/ShermanMayor.html.

³ President George W. Bush, Address to the Nation (Jan. 10, 2007), available at <http://georgewbush-whitehouse.archives.gov/news/releases/2007/01/20070110-7.html>. See also Major Joshua F. Berry, Book Review, *ARMY LAW*, Apr. 2010, at 70 (reviewing THOMAS E. RICKS, *THE GAMBLE: GENERAL DAVID PETRAEUS AND THE AMERICAN MILITARY ADVENTURE IN IRAQ, 2006–2008* (2009)).

⁴ See, e.g., Fact Sheet: Success of the Surge Allows Political Improvements in Iraq, Office of the Press Secretary, OFFICE OF THE PRESS SECRETARY (Oct. 15, 2008) (using the word “surge” to describe troop increases in Iraq), available at <http://georgewbush-whitehouse.archives.gov/news/releases/2008/10/20081015-7.html>.

⁵ See, e.g., Andy Zelleke and Robert Dujarric, Op-Ed., *The Success of That Surge*, *BOS. GLOBE*, July 31, 2008, at A9 (listing some examples of arguments for and against “the Surge”).

In *The Good Soldiers*, David Finkel leaves behind the debate about whether the escalation was right or wrong, and instead focuses on the effects of that escalation on the soldiers who had to make “the surge” work.⁶ Finkel follows the 2-16th Infantry Battalion, based in Fort Riley, Kansas, from January 2007 till June 2008, including eight months embedded with the unit in Iraq, and visits to Brooke Army Medical Center (BAMC), the National Naval Medical Center (NNMC), Walter Reed Medical Center (WRMC), and Fort Riley.⁷ His observations paint a somber and compelling picture of souls forever changed by the death of comrades, joyful optimism crushed by bitter reality, and family relationships challenged to the breaking point by the distance and trauma of war.

That somber picture provides lessons that can assist judge advocates in dealing professionally with legal assistance, criminal justice, and Law of War issues. That same somber picture can also assist judge advocates personally in preparing for the effect of combat deployment on their own mental health and close relationships.

II. Background

David Finkel is currently the enterprise editor for THE WASHINGTON POST and has worked there since 1990.⁸ During that time, he has reported for THE WASHINGTON POST on the conflicts in Kosovo, Iraq, and Afghanistan.⁹ In 2006, he received the Pulitzer Prize for explanatory reporting about efforts by the United States to facilitate democracy in Yemen.¹⁰ His plan in writing *The Good Soldiers* was simply to follow an infantry battalion during “the surge,” and he wondered why no one had done it before.¹¹ “But after the fourth or fifth rocket attacks, I realized why nobody had done it.”¹²

III. Analysis

Finkel begins by introducing the members of the 2-16th as they prepare to deploy to Iraq. The most central character is Lieutenant Colonel (LTC) Ralph

⁶ FINKEL, *supra* note 1, at 285 (“From the beginning, I explained to them that my intent was to document their corner of the war, without agenda.”).

⁷ *Id.*

⁸ About the Author: David Finkel, <http://www.washingtonpost.com/wp-srv/special/opinions/outlook/the-good-soldiers/> (last visited June 14, 2012).

⁹ *Id.*

¹⁰ *Id.*

¹¹ Collette Bancroft, *David Finkel Gives Voice to the Infantrymen in “The Good Soldiers,”* TAMPA BAY TIMES, Sep. 20, 2009, available at <http://www.tampabay.com/features/books/david-finkel-gives-voice-to-the-infantrymen-in-the-good-soldiers/1037017>.

¹² *Id.*

Kauzlarich, the battalion commander.¹³ Lieutenant Colonel Kauzlarich is a continuously positive leader whose motto is “It’s all good.”¹⁴ That optimism would remain throughout the deployment, but it would be severely tested,¹⁵ and not always appreciated by the men serving under him.¹⁶ Still, that optimism was not blind as LTC Kauzlarich recognized, “This is probably going to change me.”¹⁷

At first glance, this introduction seems brief and rather insignificant. The entire recounting takes up only a dozen pages of Finkel’s book.¹⁸ However, within those twelve pages rests the book’s first important lesson for judge advocates—the importance of getting one’s affairs in order, both legally and psychologically.

Finkel shows the soldiers laying out how they wish to be laid to rest, getting powers of attorneys and wills, and being briefed on stress management.¹⁹ Finkel describes how the soldiers do this with a mixture of “nonchalance”²⁰ and “eager”²¹ energy. What also comes through in his writing is the calming reassurance these rituals give the soldiers that their affairs are in order and steps have been taken to provide for their loved ones.²² Judge advocates must not view preparing wills and powers of attorney as a mindless, repetitive task but instead as a sacred duty to help soldiers feel secure that their possible death will not leave their families unsupported.

“If you are not ready to die, you need to be. If you are not ready to see your friends die, you need to be.”²³ These parting words from the chaplain send the members of the 2-16th off to Iraq, and, for a time, such ominous preparation was not necessary. For roughly two months, whether through luck or training, the 2-16th found weapons before they could be used against them, and avoided the rounds and improvised explosive devices (IED) sent their way.²⁴ Sadly, their luck would not last.

¹³ FINKEL, *supra* note 1, at 5.

¹⁴ *Id.* at 5.

¹⁵ *See, e.g., id.* at 7; *see also id.* at 142–147.

¹⁶ *Id.* at 3; *see also id.* at 112.

¹⁷ *Id.* at 7.

¹⁸ *Id.* at 3–16.

¹⁹ *Id.* at 11–12.

²⁰ *Id.* at 13.

²¹ *Id.* at 13.

²² *Id.* at 13–14.

²³ *Id.* at 12.

²⁴ *Id.* at 19.

The men of the 2-16th learned that explosions kill “good soldiers” too.²⁵ Private First Class (PFC) Jay Cajimat was killed when an IED exploded next to his vehicle.²⁶ Finkel eventually focuses on the impact of PFC Cajimat’s death on the unit,²⁷ but a side-step in the story provides the next lesson that judge advocates can learn about the impact of war—you do not have to be injured to be affected by serving in a combat zone.

“I don’t read the letters. I don’t look at the pictures. It keeps me sane.”²⁸ Finkel hears these words while talking to the soldiers who work in Mortuary Affairs.²⁹ Their job is to search the remains of the dead for personal items like pictures and letters to family members.³⁰ As Finkel continues to talk to the soldiers, one soldier chides another who has gotten too curious, “Hey man. Don’t read no (sic) letters.”³¹ The mental health of combat-hardened soldiers is clearly a concern. However, as suicide rates in the United States Army reach a thirty-year high,³² judge advocates must remember that “non-combat” soldiers, like themselves and their paralegals, also need to be observed for any psychological problems resulting from being in a combat environment.

The next lesson for judge advocates comes from a combination of the introduction of counterinsurgency (COIN) doctrine to infantry units³³ and the conduct of the enemy.³⁴ Major (MAJ) Brent Cummings, the battalion’s executive officer, summarizes the quandary of an infantry battalion in Iraq this way, “Our task and purpose is to close with and destroy the enemy. We are the only force designed for this. Armor stands off and they kill from a distance. Aviation kills from a distance. The infantryman goes in and kills with his hands, if necessary.”³⁵ The difficulty of the demands of this war, as MAJ Cummings

²⁵ See *id.* at 19.

²⁶ *Id.* at 19-20.

²⁷ *Id.* at 22-24 (“Tonight, we take the time to honor Task Force Ranger’s first loss, an unfortunate loss that in a special way made us as an organization whole.” (quoting LTC Kauzlarich’s speech at PFC Cajimat’s memorial service)).

²⁸ *Id.* at 21.

²⁹ *Id.* at 20-21.

³⁰ *Id.* at 21.

³¹ *Id.*

³² Julian E. Barnes and Jia-Rui Chong, *Army Suicide Rate Hits A Three-Decade High, Officials Say*, L.A. TIMES, Jan. 30, 2009, available at <http://articles.latimes.com/2009/jan/30/nation/na-army-suicides30>.

³³ See U.S. DEP’T OF ARMY FIELD MANUAL, 3-24, COUNTERINSURGENCY para. 1-2 (15 Dec. 2006) [hereinafter FM 3-24] (“*Counterinsurgency* is military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency (JP 1-02).”).

³⁴ See, e.g., FINKEL, *supra* note 1, at 54–55.

³⁵ *Id.* at 27.

saw it, was that, instead of killing the enemy, the war required “drinking chai, handshaking, being political.”³⁶

These infantrymen were faced with a war that required trained killers to become politicians. They also faced an enemy that fought from the shadows and used IEDs and sneak attacks to fight, which led to “suspicion in 360 degrees.”³⁷ This new type of conflict led to a war that moved in the minds of the men of the 2-16th from “beginning clarity” to “more maybes.”³⁸ Compounding that uncertainty was the anger that rose with each IED, suicide bombing and sniper attack that left another soldier injured or killed, and resulted in one non-commissioned officer (NCO) saying, “I hate all these motherfuckers.”³⁹

Such confusion and anger may or may not be conducive to an effective implementation of COIN strategy, but it can be conducive to Law of War violations and criminal conduct. The role of the judge advocate in keeping Law of War training fresh, understandable, and constant cannot be overstated in such an environment. Judge advocates cannot look at teaching about Law of War, rules of engagement, and other similar classes as just another opportunity to toss together a few slides and spend fifty minutes teaching a class. Effective training could be the difference between no or minor issues and another Abu Ghraib situation.⁴⁰

Between fighting insurgents and dealing with politicians, the leadership also had to worry about things like “Bob.” “Bob” was not the name of a person but the nickname given to an unidentified, dead Iraqi man found bobbing in a sewage drain located in the middle of a factory that the unit wanted to turn into a forward base of operations.⁴¹ The proposed purpose of this base was to stop the insurgents who were building bomb-making materials in the factory, and to use the base to help bring the area under control.⁴²

Major Cummings anguished over how to get “Bob” out of the sewage as he felt he could not ask an American soldier to go into what was effectively a sewage-filled grave, and yet he also could not find a way to fund the expense of paying an Iraqi to do it.⁴³ Insurgents eventually solved the “Bob” problem for

³⁶ *Id.* at 28.

³⁷ *Id.* at 37.

³⁸ *Id.* at 70.

³⁹ *Id.* at 51.

⁴⁰ See Major General Antonio M. Taguba, Army Regulation 15-6 Investigation of the 800th Military Police Brigade, at 19, para. 12 (May 2004), available at <http://news.findlaw.com/hdocs/docs/iraq/tagubarpt.html#ThR1.9>.

⁴¹ FINKEL, *supra* note 1, at 45-46.

⁴² *Id.* at 46.

⁴³ *Id.* at 47-48.

him by destroying the factory.⁴⁴ However, the use of the factory as a forward base of operations was lost, and the next lesson for judge advocates is clear—quick and effective solutions to problems concerning contract and fiscal law can be a great combat multiplier.

Imagine that MAJ Cummings went to his judge advocate with this problem. Now imagine that judge advocate was able to quickly find a way to fund an Iraqi removing this body. The 2-16th might have been able to get the body cleared out more quickly. The factory might have been secured before the insurgents could blow it up. Major Cummings might have had one less combat stressor occupying his time and thus could have returned his focus to main combat operations. A forward base might have resulted in more intelligence or better security. American or Iraqi lives could have been saved. All of this might have been possible because of a judge advocate. However, it did not happen.

A final lesson for judge advocates from Finkel's book flows from the last half of *The Good Soldiers*—many soldiers start off as good soldiers but trauma, death, and loss in war transform them greatly.⁴⁵ This is a particular consideration for judge advocates in criminal justice billets with the responsibility for advising commanders on courts-martial, administrative separations, and non-judicial punishments.

Finkel best shows this lesson in two areas. First, in the eulogies given after the death of a member of the 2-16th, Finkel shows the raw pain felt at the loss of a brother-in-arms describing one eulogy as “so overflowing with hurt it was like listening to the exact moment of someone being transformed by heartbreak.”⁴⁶ Second, Finkel reveals a fundamental shift in the personalities and thought-processes of many of the men of the 2-16th.

He does this through showing the inner thoughts of the soldiers and their dealings with their families. Many of the soldiers speak of “slide shows” in their head showing soldiers in flames or other disturbing images repeated over and over again.⁴⁷ Nearly all describe frustrations and disruptions in the patterns

⁴⁴ *Id.* at 50.

⁴⁵ See, e.g., Fernanda Santos, *Sergeant Fled Army, but Not the War in His Head*, N.Y. TIMES, Nov. 18, 2007, available at http://www.nytimes.com/2007/11/18/nyregion/18awol.html?_r=1&ref=posttraumatic_stress_disorder (showing a command deciding between court-martial and administrative discharge for a soldier possibly suffering from post-traumatic stress disorder (PTSD)).

⁴⁶ FINKEL, *supra* note 1, at 111.

⁴⁷ *Id.* at 122.

of their personal relationships with unplanned weddings,⁴⁸ spending sprees,⁴⁹ secrets kept,⁵⁰ and even good relationships challenged by disconnect.⁵¹

Trial counsel should consider examining packets and talking to commanders about how soldiers accused of misconduct differ from before deployment to after deployment in considering decisions on adverse actions. Alternatives to court-martial should be considered where mental health issues are suggested. Defense counsel absolutely should look beyond the act committed by a soldier and see if an accused has been diagnosed with a combat-related mental illness, or see if he should be examined for such an illness.

Judge advocates advising commanders should also consider reminding commanders about the importance of identifying, treating, and de-stigmatizing combat stress. Lieutenant Colonel Kauzlarich reluctantly saw a combat stress specialist at one point during his tour.⁵² However, at other times, he still referred to many soldiers reported to have combat stress issues with the diagnosis of “[H]e’s just a pussy.”⁵³

IV. Conclusion

The Good Soldiers is interesting because it vividly describes the journey of the men of the 2-16th as they fight and live through “the Surge.” This book can be read for the deep insights it gives into the lives of individual soldiers, or for the graphic and disturbing imagery which places the reader right next to LTC Kauzlarich and his men—“I remember the blood was coming off his head and coming into my mouth. I couldn’t get the taste out. That iron taste. I couldn’t drink enough Kool-Aid that day.”⁵⁴ Even though Finkel neither explicitly condones nor condemns “the surge,” a reader can create from *The Good Soldiers* arguments both for the futility of the operation, and the indelible spirit of the soldiers of the United States Army.

However, while all of those things make Finkel’s work interesting and worth reading in their own right, none are what makes this book important for judge advocates to read. What makes this book a necessity for every judge advocate are the lessons that can be learned from *The Good Soldiers*.

⁴⁸ *Id.* at 184-85.

⁴⁹ *Id.* at 181.

⁵⁰ *Id.* at 195-96.

⁵¹ *Id.*

⁵² *Id.* at 186-87.

⁵³ *Id.* at 187.

⁵⁴ *Id.* at 53.

These lessons, from the impact of war on soldiers psychologically to the critical role of judge advocates in assisting commanders in dealing with the fallout of that impact to the function of judge advocates as combat multipliers, will help judge advocates perform their role in a combat environment effectively and aid the unit in accomplishing the mission and taking care of soldiers.

Read *The Good Soldier* for those lessons, even as you enjoy it for its effective writing, colorful imagery, and unvarnished examination of fifteen months in the life of a “surge” infantry battalion.

INFORMATION FOR AUTHORS

Authors are invited to discuss prospective articles with the *Naval Law Review* Editor-in-Chief at (401) 841-3800 ext. 145 or DSN 841-3800 ext. 145 or by writing to Editor-in-Chief, *Naval Law Review*, Naval Justice School, 360 Elliot ST, Newport, RI 02841-1523.

The Editor-in-Chief, in conjunction with article editors, carefully reviews each manuscript for clarity, accuracy, and scholarly merit. The Editor-in-Chief reserves the right to make editorial changes to a manuscript selected for publication. Manuscripts will not normally be altered in a manner inconsistent with the substance of the author's position. Where practical, the board will notify the author of any substantive changes before publication. There are no specific guidelines on manuscript length; brevity is not an obstacle to publication of a quality manuscript.

Manuscripts must be submitted in Microsoft Word format. Authors should include an abstract of the proposed article, a short biography, and a statement as to whether the manuscript has been submitted elsewhere for publication. Per current directives, authors are solely responsible for security review. Authors may take a different position from that held by the government. When the author purports to state the views of the Department of the Navy or another governmental entity, however, security review is essential to ensure that the official position is stated accurately. No compensation can be paid for any articles published.

Articles should conform to the current edition of *The Bluebook: A Uniform System of Citation* (19th ed.) ("*The Bluebook*") and the *Military Citation Guide* (18th ed.). Authors should consult the *U.S. Government Printing Office Style Manual* (rev. ed. 2008), on matters not addressed in *The Bluebook*.

